T.C.
MİLLİ EĞİTİM BAKANLIĞI

MEGEP

(MESLEKİ EĞİTİM VE ÖĞRETİM SİSTEMİNİN
GÜÇLENDİRİLMESİ PROJESİ)

BİLİŞİM TEKNOLOJİLERİ

TCP/IP TAŞIMA VE UYGULAMA KATMANI

ANKARA 2008

Milli Eğitim Bakanlığı tarafından geliştirilen modüller;

- Talim ve Terbiye Kurulu Başkanlığının 02.06.2006 tarih ve 269 sayılı Kararı ile onaylanan, Mesleki ve Teknik Eğitim Okul ve Kurumlarında kademeli olarak yaygınlaştırılan 42 alan ve 192 dala ait çerçeve öğretim programlarında amaçlanan mesleki yeterlikleri kazandırmaya yönelik geliştirilmiş öğretim materyalleridir (Ders Notlarıdır).
- Modüller, bireylere mesleki yeterlik kazandırmak ve bireysel öğrenmeye rehberlik etmek amacıyla öğrenme materyali olarak hazırlanmış, denenmek ve geliştirilmek üzere Mesleki ve Teknik Eğitim Okul ve Kurumlarında uygulanmaya başlanmıştır.
- Modüller teknolojik gelişmelere paralel olarak, amaçlanan yeterliği kazandırmak koşulu ile eğitim öğretim sırasında geliştirilebilir ve yapılması önerilen değişiklikler Bakanlıkta ilgili birime bildirilir.
- Örgün ve yaygın eğitim kurumları, işletmeler ve kendi kendine mesleki yeterlik kazanmak isteyen bireyler modüllere İnternet üzerinden ulaşılabilirler.
- Basılmış modüller, eğitim kurumlarında öğrencilere ücretsiz olarak dağıtılır.
- Modüller hiçbir şekilde ticari amaçla kullanılamaz ve ücret karşılığında satılamaz.

İÇİNDEKİLER

AÇIKLAMALAR ii
GİRİŞ 1
ÖĞRENME FAALİYETİ–1 3
1. TCP/IP TAŞIMA KATMANI 3
1.1. Taşıma Katmanı 4
1.2. Eş Sistemler Arası Bağlantı Kurma 6
1.3. Taşıma Katmanı Protokolleri 7
1.3.1. TCP 7
1.3.2. UDP 26
1.3.3. TCP ve UDP Port Numaraları 29
UYGULAMA FAALİYETİ 36
ÖLÇME VE DEĞERLENDİRME 38
ÖĞRENME FAALİYETİ–2 40
2. TCP/IP UYGULAMA KATMANI 40
2.1. TCP/IP Uygulama Katmanı 40
2.2. UYGULAMA KATMANI PROTOKOLLERİ 40
2.2.1. DNS 42
2.2.2. FTP VE TFTP 48
2.2.3. HTTP (HyperText Transfer Protocol) 54
2.2.4. SMTP (Simple Mail Transfer Protocol) 60
2.2.5. SNMP (Simple Network Management Protocol) 65
2.2.6. Telnet 70
UYGULAMA FAALİYETİ 72
ÖLÇME VE DEĞERLENDİRME 74
MODÜL DEĞERLENDİRME 76
CEVAP ANAHTARLARI 78
KAYNAKÇA 79

AÇIKLAMALAR

KOD	**481BB0052**
ALAN	**Bilişim Teknolojileri**
DAL/MESLEK	**Ağ İşletmenliği**
MODÜLÜN ADI	**TCP/IP Taşıma ve Uygulama Katmanı**
MODÜLÜN TANIMI	Bilgisayar ağlarında TCP/IP'nin taşıma katmanı ve uygulama katmanının tanıtıldığı öğrenme materyalidir.
SÜRE	40/24
ÖN KOŞUL	Alt Ağlar modülünü tamamlamış olmak
YETERLİK	TCP/IP taşıma ve uygulama katmanını kullanmak
MODÜLÜN AMACI	**Genel Amaç** Öğrenci bu modül ile gerekli ortam sağlandığında, TCP/IP taşıma ve uygulama katmanını kullanabilecektir. **Amaçlar** ci; **1.** Taşıma katmanının işlevini ve protokollerini kavrayarak, portları test edebileceksiniz. **2.** Uygulama katmanını işlevini kavrayarak, uygulama katmanının protokollerini uygulayabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	Ağla birbirine bağlı bilgisayar laboratuarı, yönlendirici ve modem.
ÖLÇME VE DEĞERLENDİRME	➢ Her faaliyet sonrasında o faaliyetle ilgili değerlendirme soruları ile kendi kendinizi değerlendireceksiniz. ➢ Modül sonunda uygulanacak ölçme araçları ile modül uygulamalarında kazandığınız bilgi ve beceriler ölçülerek değerlendirilecektir.

GİRİŞ

Sevgili öğrenci;

Bilgisayarlar gelişimlerinde, geçmişlerinden bugüne çok fazla yol alarak artık yaşamımızın her alanına girdi. Abaküs halindeki basit makineler şimdilerde ellerimizde taşıdığımız avuç içi bilgisayarlara dönüştü ve bilgisayarlar yaşamımızın ayrılmaz parçası haline geldi.

Diğer yandan gelişen bir sektör de iletişim oldu. Önceleri santral başındaki çalışanın verdiğimiz numarayı bağlamasını beklerdik. Hatlar meşgul olduğu için telefon başında saatlerce bağlanmayı beklerdik. Şimdi o günlerden geriye ne kaldı? Cep telefonları hepimizin ceplerine girdi.

Gelişen bu iletişim ortamında haberleşme dışında bilgilerin de paylaşılması ihtiyacı oluştu. Nasıl insanların bir şeyler paylaşmak için birbirlerini arayıp konuşmaları gerekiyorsa, bilgisayarların işledikleri bilgileri paylaşmak için birbirleriyle iletişim kurmaları gerekiyor. Bilgisayarlar arasına, evlere bağlanan telefon kablolarına benzer kablolar bağlandı. Fakat bilgisayarlar nasıl konuşacaklardı?

Nihayet bilgisayarların konuşup iletişim kurmaları için farklı bilgisayar dilleri bulundu, bilgiler paylaşılmaya başlandı. Önceleri, kullandıkları sistem, dil birbirinden farklı olduğu için yalnızca aynı dili konuşan, aynı tip bilgisayarlar anlaşabiliyorlardı.

İnternet ortamında birçok bilgisayar var. Nasıl tüm dünyada ingilizce ortak dil olarak belirlenmiş, farklı insanlar anlaşabilmek için ingilizce konuşuyorsa, farklı sistemler kullanan, farklı diller konuşan bilgisayarların da birbirleri ile iletişim kurmaları için ortak bir lisan geliştirildi. Böylece ellerimizde taşıdığımız küçük bilgisayarlardan devasa sunucu bilgisayarlara kadar hepsi haberleşebilir, hepsi bilgilerini paylaşabilir hale geldiler. Artık çok güvenli banka sistemleri ile evlerimizde kullandığımız basit kişisel bilgisayarlar iletişim kurabiliyor, banka işlemlerimizi evimizin rahatlığında yapabiliyoruz.

İşte bu iletişim ortamını sağlayan ortak lisanın adı TCP/IP olarak belirlenmiş, bütün sistemlerde tanınmıştır. Bilgisayarlar iletişim kurarken bu dilin kurallarına göre konuşmak, bu dilin kurallarına göre iletişim kurmak zorundadır.

Bu modül sonunda bu dilin kuralarını ve nasıl konuşulduğunu, bilgisayarların birbirlerine bilgileri nasıl gönderdiğini, en çok kullandığınız e-postaların nasıl iletildiğini öğreneceksiniz. Evinizdeki bilgisayarın, dünya üzerinde nerde olduğu hakkında bir fikrinizin bile olmadığı bilgisayarları bulup aradığınız bilgileri size nasıl taşıdığını öğreneceksiniz.

ÖĞRENME FAALİYETİ-1

AMAÇ

Taşıma katmanının işlevini ve protokollerini kavrayarak, portları test edebileceksiniz.

ARAŞTIRMA

- İInternet ağı, protokol, port kavramlarının neler olduğunu araştırınız. Edindiğiniz bilgileri sınıfta paylaşınız.

1. TCP/IP TAŞIMA KATMANI

Bilindiği gibi gerek küçük ağlarlar (LAN) üzerindeki, gerek geniş ağlar (WAN) üzerindeki, gerekse İnternet üzerindeki bütün cihazların birbirleri ile konuşmalarını sağlayan protokol ailesidir. LAN ve WAN için tasarlanmıştır ve belirli bir sahibi yoktur.

TCP ve IP ağ üzerinde gelen-giden, her iki yönde bilgi akışını kontrol eder. IP bilgilerin ne olduğuyla ilgilenmez. Sadece paketlenmiş bilgileri diğer noktaya yönlendirir. Bunu bir mektup olarak düşünürsek, IP zarfın üzerine gönderilecek olan adresi yazar. TCP ise paketleri gönderir ve yerine ulaşıp ulaşmadığını kontrol eder.

Araştırmacıların belli başlı hedefleri vardı ve bu hedefleri gerçekleştirmek için TCP/IP protokollerini geliştirmişlerdir. TCP/IP'nin gerçekleştirdiği bu hedefler:

- Bütün üretici firmaların ürettikleri ağ araçlarını kullanabilir.
- Ana bilgisayar, masaüstü, diz üstü bilgisayarlar, el bilgisayarları ve hatta cep telefonları arasında iletim yapabilir.
- Farklı işletim sistemleri arasında veri alışverişi yapabilir.
- Unix sistemlerine uyumludur.
- İnternet üzerinde kullanılabilir.

TCP/IP, OSI (Open System Interconnection) gibi üst üste sıralanmış katmanlardan oluşur. Fakat TCP/IP protokol grubu DOD (Department Of Defense) modelini referans almıştır. TCP/IP OSI modelinden önce geliştirilmiştir ve OSI modelinin yedi katmanına karşılık TCP/IP dört katmana sahiptir.

4	UYGULAMA	Kullanıcı işlemleri ile alt seviye protokolleri arasında bir arayüzdür.
3	TAŞIMA	Kaynak ve hedef portlar arası bağlantıları kontrol eder.
2	İNTERNET (AĞ)	Hedef ve iletim adreslerini işler, yönlendirme yapar.
1	FİZİKSEL (AĞ ARAYÜZ)	Donanım adreslerini verir, LAN ve WAN'a fiziksel bağlantı yapar.

Tablo 1: TCP/IP Katmanları

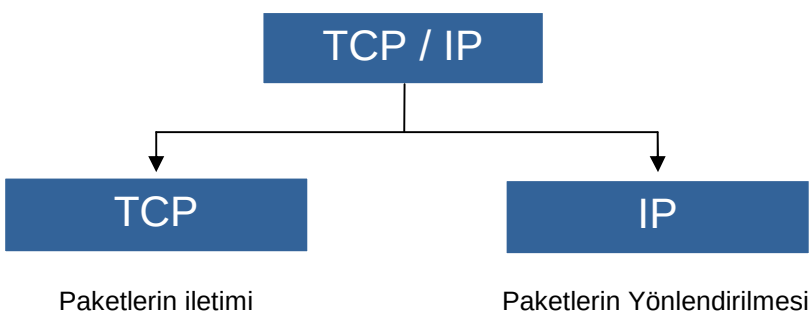
TCP/IP Protokol Grubu				
IP Adresleme	Ağ Arayüz Katmanı	Internet (Ağ) Katmanı	Taşıma Katmanı	Uygulama Katmanı
ALT AĞLAR	ETHERNET	ARP	TCP	DNS
YAYIN	Token Ring	RARP	UDP	FTP, TFTP
Çoklu Yayın	FDDI	IP		HTTP
	ATM	ICMP		SMTP
				SNMP
				TELNET

Tablo 2: TCP/IP Protokolleri

Sevgili öğrenci; bu bölümde taşıma katmanı ve bu katmana ait protokolleri öğreneceksiniz.

1.1 Taşıma Katmanı

TCP/IP, temelde TCP (Transmission Control Protocol – İletim Kontrol Protokolü) ve IP (Internet Protocol – İnternet Protokolü) olmak üzere iki ana protokolden oluşur. Bilgiler paketlenirler ve TCP bu paketlerin iletilmesinden, IP ise bu paketlerin yönlendirilmesinden sorumludur. Taşıma katmanında TCP ve UDP(User Datagram Protocol), ağ katmanında ise IP kullanılır.



Şekil 1: İki Temel TCP/IP Protokolü

Bu bölümde taşıma katmanı üzerinde durulacaktır.

TCP/IP'de üçüncü katman olan taşıma katmanının temel görevi adından da anlaşıldığı gibi, paketler haline getirilen bilgileri iletmektir. İletme işleminde biri gönderen, diğeri alan olmak üzere iki uç arasında bir bağlantı kurulur. Bilgiler paketler haline dönüştürülür ve gönderen uçtan alıcı uca aktarılır.

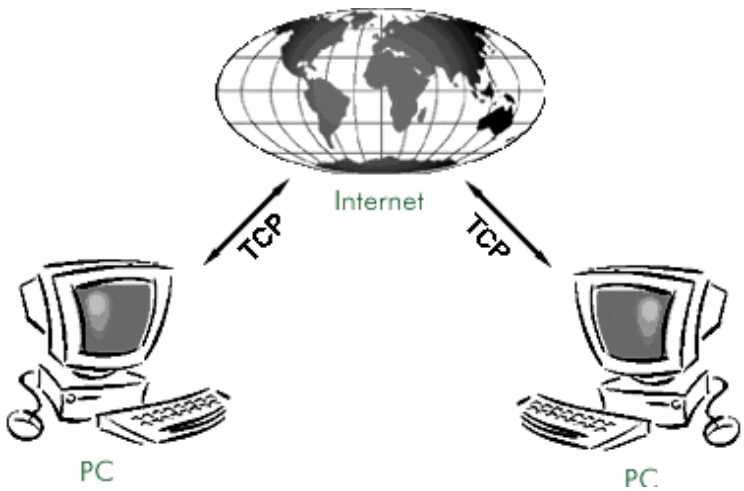
Bu aktarma işleminde öncelikle eş sistemler arasında bir bağlantı kurulur. Daha sonra bilgi paketlerini taşıma işlemine geçilir.

Taşıma işleminde biri TCP değeri UDP olmak üzere iki teknik kullanır. Bu tekniklerden hangisinin kullanılacağına ise taşınacak olan bilgi tipine göre karar verilir. Eğer taşınacak bilgi değerli, hatasız iletilmesini istiyorum, çok hızlı olmasa da olur ama garantili iletilsin deniliyorsa TCP, taşıma sırasında kayıplar çok önemli değil, hızlı bir iletim istiyorum deniliyorsa UDP kullanılır.

Taşıma katmanı protokolleri TCP ve UDP protokollerinin her ikisini de kullanır. Bu nedenle bilgi paketleri için her zaman iletim garantisi vermez.

1.2. Eş Sistemler Arası Bağlantı Kurma

Bilgi paketlerinin iletilebilmesi için öncelikle kaynak ve hedef sistemler eşleştirilerek aralarında bir bağlantı kurulmalıdır.



Şekil 2: İnternet Üzerinde TCP Bağlantısı

Telefonla birilerini ararken önce numara çevirirız. Hat meşgul değilse karşı tarafın telefonu çalar. Aradığımız kişi telefonu açtığı anda arada bağlantı kurulmuş olur. Artık aradığımız kişiye söylemek istediğimiz sözleri iletiriz.

TCP/IP'de de durum bundan farklı değildir. Burada da kaynak ve hedef sistem olmak üzere iki taraf vardır. Kaynak sistem hedef sisteme bağlantı isteğinde bulunur. Kaynak, hedef sistemin bağlantıya hazır olmasını bekler. Hedef sistem bağlantıya hazır ise bu isteği kabul eder. Böylece arada bir bağlantı kurulur.

Bu bağlantı ilerleyen sayfalarda "Bağlantı Kurulumu" başlığı altında detaylı bir şekilde anlatılacaktır.

1.3. Taşıma Katmanı Protokolleri

Taşıma katmanında bilgi paketlerini taşımak için TCP ve UDP olmak üzere iki farklı protokol kullanır. TCP bağlantılı, UDP bağlantısızdır. Bunun anlamı; TCP kaynak sistemden hedef sisteme gönderilen bilgilerin yerine hatasız ulaşıp ulaşmadığını kontrol eder. Hatalı ulaşan paketleri tekrar göndererek hedefe ulaştığından emin olur. UDP'de ise durum farklıdır. Paketler gönderilir ve karşı tarafa hatasız ulaşıp ulaşmadığı ile ilgilenilmez. Kontrol mekanizması kullanılmadığı için hızlı bir iletim yapılır. TCP'de iletim garantili iken UDP hatalı iletim yapabilme ihtimali olması nedeniyle garantili değildir.

Bu başlık altında TCP ve UDP protokollerinin nasıl işlediğini ayrı ayrı inceleyelim.

1.3.1. TCP

TCP birbirinden farklı, çok çeşitli ağ uygulamalarını destekleyen protokollerin katman hiyerarşisi içerisine uyacak şekilde dizayn edilmiş, uçtan uca (alan ve gönderen uçlar) güvenilir iletim yapan bağlantılı (Connection Oriented) bir protokoldür. Yapıları birbirinden farklı ağlar üzerinde de iletim yapabilir.

TCP, bu katmanlı protokol mimarisinde bir tarafında uygulama katmanı ile diğer tarafında bulunan İnternet Protokolü (ağ katmanı) arasındaki bağlantıyı sağlayan protokol olarak bir arayüz görevi yapar. Ayrıca her türlü ağ uygulamalarında çalışabilir.

TCP'nin temel görevi; güvenilirlik, kaynak ve hedef uygulama çiftleri arasında güvenli mantıksal bağlantılar kurmaktır. Bu protokolden, İnternetin güvenilir olmayan ortamında belirli alanlarda başarı sağlaması beklenmektedir. Bu alanlar:

- Temel Veri Transferi
- Güvenilirlik
- Akış Kontrolü
- Veri Seçiciliği
- Bağlantılar
- Öncelik ve Güvenlik
- TCP İletim İşlemi Modeli
- Arayüzler

Şimdi de TCP'nin sıralanan bu başlıkların her birindeki temel işlevlerini inceleyelim.

1.3.1.1. Temel Veri Transferi

TCP, iki uçtaki farklı kullanıcının iletmek istedikleri verilerin İnternet ortamında transferi için bilgi paketlerinin bazı bölgelerini numaralandırıp sürekli akış halinde, her iki yönde de iletebilir. Gönderen tarafta, üst katmandan gelen paketlenmiş bilgilere TCP başlıklarını ekleyerek bir alt seviyedeki ağ (IP) katmanına iletir. Alıcı tarafta ise alt katmandan (IP) aldığı paketlerdeki TCP başlıklarını çıkartarak üst katmana iletir. Böylece her iki taraftaki TCP birlikte çalışarak alıcından kullanıcıya veri iletimi yapılmış olur.

Bazen kullanıcılar TCP'ye gönderdikleri verilerin tamamının iletildiğinden emin olmak isterler. Bu amaçla gönderen kullanıcının verilerinin hedef kullanıcıya iletildiğini garanti etmek için bir iletim (push) fonksiyonu tanımlanmıştır. Bu fonksiyon bilgilerin alıcı noktaya ulaştığını TCP'ye bildirir.

TCP Full-Duplex iletim kullanır. Full-Duplex iletimde gönderici ve alıcı aynı anda birbirlerine bilgi gönderebilir. Böylece gönderici veri paketlerini gönderirken alıcı da aynı anda kontrol bilgisi gönderebilir.

1.3.1.2. Güvenilirlik

TCP hasar görmüş, kaybolmuş, iki kez gönderilmiş veya İnternet bağlantı sisteminden kaynaklanan bozuk iletilmiş veri paketlerini düzeltmelidir. Bu güvenilirliği sağlamak için ilettiği her veri paketine bir sıra numarası verir. Bu numaralı paketlerin herbiri için bir süre alıcı taraftaki TCP'den olumlu bir bilgilendirme (ACK-ACKNOWLEDGEMENT) bekler. Eğer bu süre içinde bilgilendirme gelmezse paketin alınmadığı varsayarak aynı numaraya ait paketi tekrar gönderir.

Alıcı tarafta ise alınan paketler hatlardaki oluşabilecek aksaklıklar nedeniyle yanlış sırada alınmış veya aynı paket iki defa gelmiş olabilir. Paket numaraları, bu olumsuzluklar nedeniyle paketlerin doğru sırayla birleştirilmesi için kullanılır. Gönderen taraftaki TCP ilettiği her pakete bir de hata kontrol bilgisi ekler. Alıcı TCP gelen paketlerden hata gördüklerini eler. Paketlerdeki sıra numarası ve ACK kullanımı ile iletim güvenilir bir şekilde yapılır.

1.3.1.3. Akış Kontrolü

Alıcı taraftaki TCP, kendisine gelen veri akış miktarını kontrol edebilir. Her ACK ile birlikte başarılı bir şekilde gelen son paketten sonra kabul edebileceği paket numaralarını gösteren bir liste penceresi gönderici taraftaki TCP'ye ileterek alabileceği veri miktarını sınırlar. Bu pencere başka paket gönderme izni almadan önce alınmasına izin verilen paketleri gösterir.

1.3.1.4. Veri Seçiciliği

TCP'nin bu iletişim yeteneklerini aynı anda birden fazla farklı uygulama ile kullanmak isteyebilirsiniz. Bu durumlara karşı TCP, her sunucu için bir port veya adres seti sağlar. İnternet ve ağ katmanlarındaki ağ ve bilgisayar adresleri vardır. Bu adreslerin birleştirilmesi ile soketler oluşturulur. Bir soket çoklu bağlantılarda eş zamanlı olarak kullanılabilir. TCP farklı bağlantı noktalarından aynı anda gelen verileri ilgili uygulamayı seçer ve bu uygulamaya gönderir.

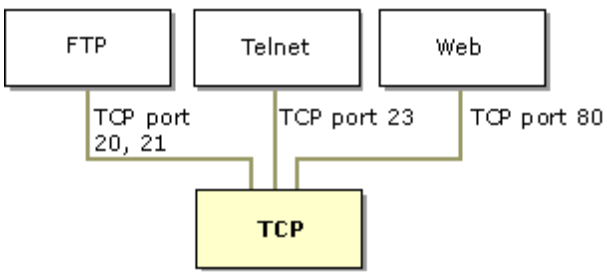
1.3.1.5. Bağlantılar

Yukarıda bahsedilen güvenilirlik ve akış kontrol mekanizmaları alıcı ve gönderici TCP'nin her ikisinin de her bir veri aktarımı için kesin durum bilgilerine bakmasını ve

incelemesini ister. Soketler, paket sıra numaraları ve pencere boyutları da dahil, bu bilgilerin kombinasyonuna bağlantı adı verilir.

TCP'nin bağlantıları iki bilgisayar arasında kurulur ve tamamen eşsizdir. TCP veri akışını sağlayabilmek için yalnızca bu iki bilgisayara özel bağlantı tanımlar. Öncelikle alıcı ve gönderen bilgisayarlardaki TCP'lerin her biri kendilerine birer port tanımlayıcı seçerler. Benzersiz bir adres olması için bu port tanımlayıcılar ile İnternet adresi birleştirilerek milyonlarca bilgisayarın birbirine bağlandığı bir ortamda tamamen eşsiz soketler oluşturulur. Bir bağlantı iki uç bilgisayarda tanımlanmış bir çift soket ile kurulur.

Portlar bilgisayarların diğer bilgisayarlarla iletişim kurdukları bağlantı noktalarıdır. Her ne kadar bu bağlantı noktalarını TCP bağımsız olarak seçse de dünya genelinde bir standart oluşturmak amacıyla bazı uygulamalar için ortak kullanılan portlar atanmıştır.



Şekil 3: TCP'de iyi bilinen ve sık kullanılan portlar

Bu port numaralarının bir standart oluşturması için tek bir merkezden belirlenip üreticilere bildirilmesi gerekir. Bilgisayarınızda bulunan yaklaşık 65.536 bağlantı noktasından 0 – 1023 arasındaki portlar İnternet Atanmış Numaralar Yetkilisi (IANA – Internet Assigned Numbers Authority) belirlemiştir. Tüm dünyada ortak kullanılır.

Port	Açıklama
1	TCP Multiplexer
20	FTP (Data)
21	FTP (Control)
23	Telnet
25	SMTP
80	http
102	X.400 Mail Sending
103	X.400 Mail Service
139	NetBIOS Session Service

Tablo 3: İyi Bilinen Bazı TCP Port Numaraları

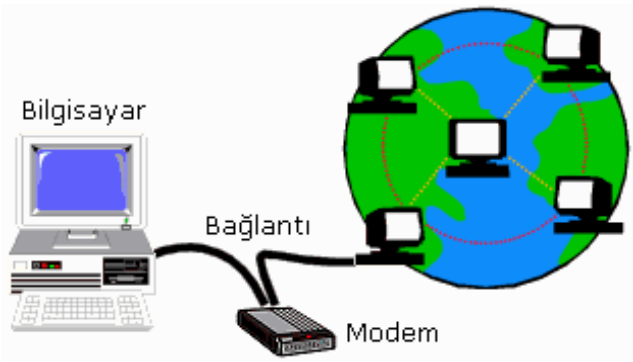
1.3.1.6. Öncelik ve Güvenlik

TCP kullanıcıları bağlantılarının önceliğini ve güvenliğini gösterebilirler. Bu özelliklere ihtiyaç duyulmadığı zamanlarda, hazırlıklar varsayılan değerler için yapılır.

Sonuç olarak; TCP İnternet bağlantı siteminde oluşabilecek hataların hepsini iletim esnasında giderir. Kararlı bir şekilde işlediği sürece, İnternet ne kadar kararsız ve güvensiz olsa da hiçbir iletim hatası bilgi paketlerinin doğru iletimini etkileyemeyecektir. TCP'nin bu tutumu ile gönderilen bilginin tamamı ya hiç iletilememiştir, iletilmişse de kesinlikle hatasız iletilmiştir.

1.3.1.7. TCP İletim İşlemi Modeli

Şimdi de TCP'nin uygulama ve İnternet katmanları arasında veri iletimini nasıl yaptığını inceleyelim.

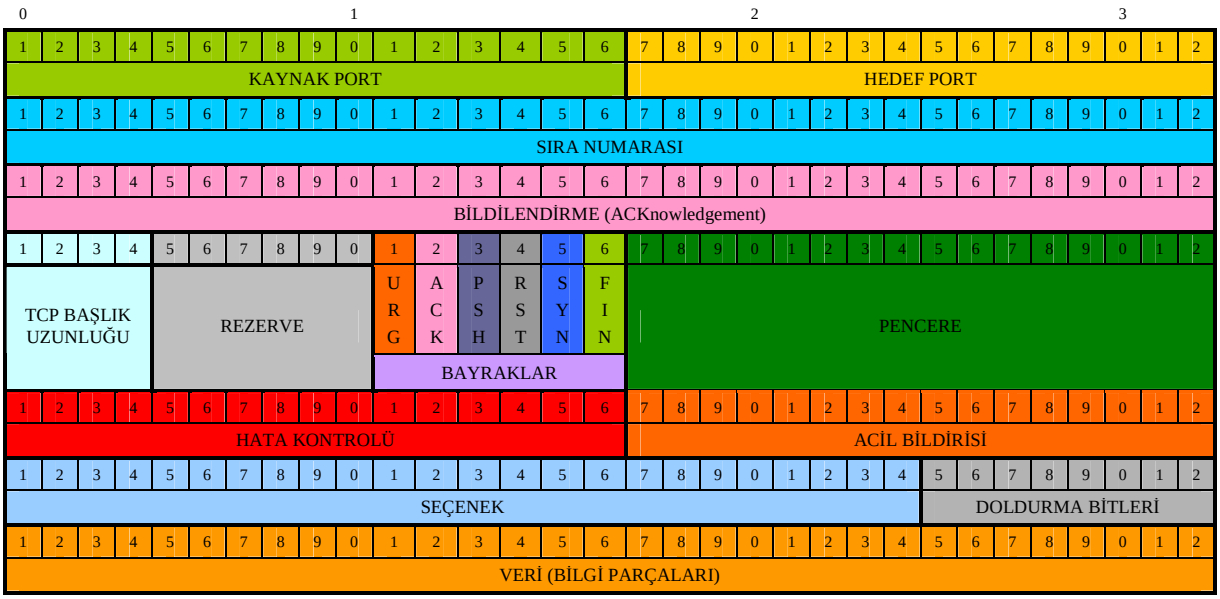


Şekil 4: İki bilgisayar arası bağlantı modeli

Kullanıcı bir bilgiyi herhangi bir uygulama programı ile gönderdiği zaman, öncelikle iki bilgisayarın karşılıklı olarak anlaşıp oturum açması gerekir. Oturum açıldıktan sonra üst katmanda bulunan bu uygulama programı, değişkenlere bilgi aktarır gibi verileri önbelleğe yerleştirir ve TCP'ye haber verir. Verilerin kendisine geldiğini haber alan TCP, bu verileri önbellekten alarak segment adını verdiğimiz küçük parçalara ayırır. Daha sonra bir altında bulunan IP katmanına bu segmentleri karşı taraftaki alıcı TCP'ye göndermesini söyler. Segmentler böylece alıcı tarafa gönderilir.

Alıcı taraftaki TCP kendisine gelen bu segmentleri açarak içinde bulunan bilgi parçalarını alır. Bu parçaları bir üst katmanında bulunan uygulama programlarına haber vererek önbelleklerine koyar. Uygulama programları bu bilgileri önbellekten alarak bilgisayar kullanıcısını bilgilendirir.

TCP sadece İnternet ortamında çalışan bir protokol değildir. Aynı zamanda yerel ağlar üzerinde de çalışır. Aynı ağ üzerindeki iki bilgisayar arasında dosya paylaşımı gibi işlemler de aynı şekilde TCP üzerinden yapılabilir.



Şekil 5: TCP Başlığı Alanları

1.3.1.7.1. Alanların Anlamları:

Kaynak Port: Gönderen bilgisayarın TCP portu.

Hedef Port: Alıcı bilgisayarın TCP portu.

Sıra numarası: TCP'nin mesajı tekrar düzgün sırada birleştirmek için kullandığı 32 bitlik bir numaradır.

Onay Numarası (Acknowledgment): Eğer ACK biti 1 ise bu alan bir sonraki pakete ait olan ve göndericinin geri bildirimle alıcının geri göndermesini beklediği sıra numarasını içerir.

TCP Başlık Uzunluğu: Bu alan 4 bit uzunluğunda ve TCP başlığında kaç adet 32 bitlik kelime olduğunu bildirir. Bu alandaki bilgi segment içinde verinin nerden başladığını gösterir. TCP başlığı 32 bit uzunluğunun katlarıdır.

Rezerve: Bu alan gelecekte olabilecek gelişmeler için kullanılmak üzere ayrılmıştır. Değeri daima "0" olmalıdır.

Bayraklar: 6 bitten oluşurlar (soldan – sağa):

- **URG :**(URGent) "1" olması Acil Göstergesi bölgesinin kullanıldığını belirtir.
- **ACK :**(ACKnowledgment) "1" olması onay alanının geçerli olduğunu gösterir.
- **PSH:**(PuSH) Gönderen TCP'nin veriyi hemen göndermesini bildirir. TCP'nin kendi öncelik sırası vardır. PuSH bayrağı bu önceliği değiştirir.

- **RST:** (ReSeT) Sorunlu veya kopmak üzere olan bağlantıları başlangıç durumuna getirmekte kullanılır.
- **SYN:** (SYNchronize) Gönderilen ilk paket ise gönderici ve alıcı tarafından kurulur. Gönderici ve alıcının sanal bağlantı isteğinde bulundukları anlamına gelir.
- **FIN:** FINish Son segmentin gönderildiğini bildirir ve bağlantı koparılabilir.

Pencere (Window): 16 bitlik bu alan onay (acknowledgment) alanından, alıcının alması beklenen alana kadar iletilecek veri baytlarının sayısını verir. Bu alan TCP'nin kayan pencere mekanizmasında akış denetimini sağlar.

Hata Kontrolü (Checksum): 16 bitlik bu alan veri transferinde başlığın bozulup bozulmadığını kontrol eder. Alıcının bu alanı kontrol ederek hatalı olduğunu tespit ettiği paketleri atar ve aynı paketin yeniden gönderilmesi ister.

Acil Göstergesi (Urgent Pointer): 16 bittir. Bu alan veri içinde acil bilginin nerede bulunacağını belirtir. Gerçekte, bu alandaki değer acil verinin son baytından sonraki değeridir. Üst katman protokolü için önemli olan verilere acil veri denir. TCP bu veri üzerinde herhangi bir işlem yapmaz. Bu alan URG bayrağı "1" ise dikkate alınır.

Seçenekler (Options): Bu alan değişken değerlidir. Eğer varsa, acil gösterge alanından sonra gelir. En çok kullanılan seçenek olan "en uzun segment boyu" seçeneğidir. İlk bağlantı kurma sırasında SYN bayrağı "1" olduğu zaman bu seçenek kullanılarak gönderilecek en uzun segment boyu verilmelidir. Aksi halde alıcı, küçük yada büyük hiçbir boyuttaki segmenti kabul etmez.

Doldurma Bitleri: Bu bitler TCP başlığının sona erip verilerin başladığını gösterir. Seçenekler alanının değişken olmasından dolayı "0" bilgileri ile doldurularak TCP başlığını 32 bitin katlarına tamamlar.

1.3.1.7.2. Terimler

TCP'nin ileri boyuttaki özelliklerine geçmeden önce bazı terim detaylarını açıklayalım. Bir TCP bağlantısı kurulurken birçok değişkene ihtiyaç duyulur. Bağlantı kaydında tutulan bu değişken değerlerine TCB (İletim Kontrol Bloğu – Transmission Control Block) denir. Gönderen ve alıcı soket numaraları, bağlantının güvenliği ve önceliği, aktif segment ve yeniden gönderilecek bilgilerin işaretçileri TCB bloğunda tutulan değişkenlerin bir kısmıdır. Bunlara ek olarak, gönderim ve alım sıra numaralarına ait birçok değişken de bu blokta tutulur.

Gönderim değişkenleri:

SND.UNA – Bilgilendirilmemiş bilgisi gönder.
SND.NXT – Bir sonrakini gönder.
SND.WND – Pencere gönder.
SND.UP – Acil işaretçisi gönder.
SND.WL1 – Güncellenen son pencere için segment sıra numarasını gönder.

SND.WL2 – Güncellenen son pencere için segment bilgilendirme numarası gönder.
ISS – Gönderim sıra numarası başlangıcı

Alım değişkenleri:

RCV .NXT – Bir sonrakini al.
RCV.WND – Pencereyi al.
RCV .UP – Acil işaretçisini al.
IRS – Alım sıra numarası başlangıcı.

Aktif segment değişkenleri:

SEG.SEQ – Segment sıra numarası.
SEG.ACK – Segment onay numarası
SEG.LEN – Segment uzunluğu
SEG.WND – Segment penceresi
SEG.UP – Segment acil işaretçisi
SEG.PRC – Segment öncelik değeri

Bir bağlantı, bağlı kaldığı süre içinde bir dizi bağlantı durumuna göre işlem yapar. Bu durumlar: LISTEN, SYN-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, TIME-WAIT ve mantıksal bir durum olan CLOSED durumlarıdır. CLOSED, bağlantıda TCB bloğu olmadığını, bu nedenle bağlantının sona erdiğini gösterdiği için mantıksaldır.

LISTEN – Herhangi bir uzak TCP yada porttan bağlantı isteği için beklendiğini gösterir.

SYN-SENT – Gönderim isteği alındıktan sonra bağlantı isteğinin uyumluluğu için beklendiğini gösterir.

SYN-RECEIVED – Alım ve gönderim isteklerinin alımından sonra bağlantı onaylama bildirimi için beklendiğini gösterir.

ESTABLISHED – Bağlantının artık açık olduğunu ve verilerin karşı tarafa gönderilebileceğini gösterir. Bağlantının veri transferi için uygun hale geldiğini gösterir bir durumdur.

FIN-WAIT-1 – Uzak TCP'den bağlantıyı koparma isteği veya bir önce gönderilmiş bağlantı kesme isteğinin onay bilgisi için beklendiğini gösterir.

FIN-WAIT-2 – Uzak TCP'den bağlantıyı koparma isteği gelemsi için beklendiğini gösterir

CLOSE-WAIT – Yerel kullanıcıdan bağlantıyı kesme isteği için beklendiğini gösterir.
CLOSING – Uzak TCP'den bağlantı kesme isteği onayı beklendiğini gösterir.

LAST-ACK – Uzak TCP'ye bir önce gönderilmiş bağlantı kesme isteğinin onayının beklendiğini (uzak TCP'nin gönderdiği bağlantı kesme isteğinin bilgilendirmesini içeren) gösterir.

TIME-WAIT – Uzak TCP'nin bağlantı kesme isteği onayını almış olduğunu kabul etmek için bekleme süresinin dolduğunu gösterir.

CLOSED – Bağlantının sonlandırıldığını gösterir.

Bir TCP bağlantısı bir durumdan diğerine geçiş işlemini olaylara cevap vererek yapar. Bu olaylar, OPEN, SEND, RECEIVE, CLOSE, ABORT ve SYS, ACK, RST, ve FIN gibi bayrakları içeren gelen segmentlere ait STATUS gibi kullanıcı çağrılarıdır.

1.3.1.7.3. Sıra Numaraları

TCP bağlantısı üzerinden gönderilen her veri baytın mutlaka bir sıra numarası vardır. Numaralanan bu baytların gönderimi sonrası her birine ait bilgilendirme gelir. Örneğin X numarasına ait bilgilendirmede bütün baytlar geldi fakat X numaralı bayt alınmadı anlamına gelir. Bu mekanizma, yeniden gönderimde öncelik sırasının belirlenmesinde etkilidir. Segment içinde baytların numaralandırılmasında ilk veri baytı başlığın hemen ardından en düşük numaralıdır ve takip eden baytlar ardışık olarak sıralanır.

Sıra numarası alanı ne kadar geniş olursa olsun sonuçta sınırlı olduğu kesinlikle unutulmamalıdır. Bu alan 0 ile 232 - 1 arasındadır. Bu nedenle sıra numaraları ile yapılacak işlemler üst sınır olan 232 ölçeğine göre yapılmalıdır. Burada dikkat edilmesi gereken nokta 232 den bir eksik olmasıdır.

TCP gönderdiği her bir segment için onay bekler. Bu onay bilgilerini işleyebilmek için şu işlemlere ihtiyaç duyar.

SND.UNA = Onaylanmamış en son segmentin numarası.
SND.NXT = Bir sonra gönderilecek segment numarası
SEG.ACK = Alıcı TCP'den onay
SEG.SEQ = Segmentin ilk sıra numarası
SEG.LEN = Segmentteki gönderilen bayt sayısı (SYS ve FIN işaretçileri dahil)

SEG.SEQ + SEG.LEN-1 = bir segmentin son sıra numarasıdır.

Aşağıdaki durum oluşursa "kabul edilebilir onay" adı verilen yeni bir onay istenir.

SND.UNA < SEG.ACK =< SND.NXT

Alıcı TCP'de bir veri alındığı zaman ise şu kontroller yapılır.

RCV.NXT = Gelen segmentte beklenen bir sonraki sıra numarası pencerenin alt sınırında mı?

RCV.NXT + RCV.WND – 1 = Gelen segmentteki son sıra numarası penceren sınırının üst limitine ulaşmış mı?

SEG.SEQ = Gelen segmentte kullanılan ilk sıra numarası.

SEG.SEQ + SEG.LEN – 1 = Gelen segmentte kullanılan son sıra numarası.

Eğer
RCV.NXT =< SEG.SEQ < RCV.NXT + RCV.WND
veya
RCV.NXT =< SEG.SEQ + SEG.LEN – 1 < RCV.NXT + RCV.WND

İse gelen segmentin geçerli bir sıra numarası alanı kullanıp kullanmadığı test edilir.

Bu testin ilk bölümünde segmentin başlangıcının pencere sınırlarından düşük olup olmadığı kontrol edilir. İkinci bölümünde ise segment birinci testten geçmiş olsa bile segment sonunun pencere sınırlarını aşıp aşmadığı kontrol edilir.

Daha kolay bir ifadeyle sıfır boyutlu pencere ve sıfır uzunluklu segmentlere göre kıyaslarsak segmentlerin kabul edilebilmeleri için dört durum vardır.

Segment Uzunluğu	Alıcı Pencere	Test
0	0	SEG.SEQ = RCV.NXT
0	>0	RCV.NXT =< SEG.SEQ < RCV.NXT + RCV.WND
>0	0	Kabul Edilemez
>0	>0	RCV.NXT =< SEG.SEQ < RCV.NXT + RCV.WND veya RCV.NXT =< SEG.SEQ+SEG.LEN–1 < RCV.NXT+RCV.WND

Tablo 4: Alıcı TCP'nin segmentleri kabul etme koşulları

Eğer alıcı pencere boyutu 0 ise ACK segmentleri haricinde hiçbir segment alıcı tarafından kabul edilmez. Peki boyutu 0 olan bir pencere nasıl gelebilir? Gönderen TCP'nin veri gönderdikten sonra yeni bir veri daha gönderir ikinci veri giderken ACK gelebilir. Bu8 ACK ile birlikte 0 uzunlukta bir pencere de gelebilir fakat veri gönderilmiştir. Alıcı bu gibi durumları tabloda gösterilen testlerden geçirir ve şartlara uymazsa paketi kabul etmez.

TCP aynı portu defalarca kullanır. Çünkü bir bağlantı iki soketle tanımlanır. Gönderici port aynı olabilir ama alıcı portlar farklıdır. Bu da bağlantıları farklı yapar. Bağlantı kurulur ve bilgiler gönderilir. Peki yukarıdaki durumlar nasıl oluşur da TCP aynı segment numarasını yada eski bir segment numarasını kullanabilir ve paketler reddedilebilir?

Bu durumlar çok hızlı bir şekilde açılıp kapatılan bağlantılarda veya bellek yetersizliğinden kaybedilen bağlantıların yeniden kurulması sonucu oluşurlar.

Kopmuş bir bağlantı üzerine yeni bir bağlantı kuruluyor olabilir. Yeni bir bağlantı yeni sıra numaraları demektir. Fakat az önce kopmuş bir bağlantıdan kalma paketler halen ağ üzerinde olabilir. Bu durumu engellemek için yeni bir bağlantı kurarken ISN (Initial Sequence Number) denilen bir sıra numarası üretici modül devreye girer. ISN 32 bitlik bir saat ile en düşük değerlikli bitleri her 4 mikro saniyede bir artırarak 32 bitlik yeni sıra numaraları üretir. Buna göre ISN'nin tam çevrimi yaklaşık 4.55 saat yapar. Maksimum segment ömrü (MSL) bu süreden kısadır. Bu nedenle ISN ürettiği numaralar ağ üzerindeki segmentlerin numaralarından kesinlikle farklı olacaktır.

1.3.1.7.4. Üç Yollu El Sıkışma

Her bağlantı için bir gönderici sıra numarası bir de alıcı sıra numarası vardır. ISN veri gönderen TCP tarafından seçilir, alıcı sıra numarası (IRS) ise alıcı TCP bağlantı kurulma aşamasında gönderici tarafından gönderilen numaralardan öğrenir.

Bir bağlantı kurulması ve başlatılması için her iki taraftaki TCP'ler birbirinin segment sıra numaralarını eşleştirmesi gerekir. Bu da bağlantı kurulum segmentlerinde taşınan SYN biti ve başlangıç sıra numarasının değişiminde yapılır. Kısaca SYN bitini taşıyan segmente SYN segmenti denir ve eşleştirilecek paket sıra numaralarını taşır. Bu nedenle bu durumu çözmek için bir paket sıra numarası seçmek bu numarayı karşılıklı değişimle eşleştirmek için uygun bir mekanizmaya ihtiyaç vardır.

Senkronizasyon için gönderen ve alan her iki tarafın da kendi sıra numaralarını birbirlerine göndermeleri ve onay almaları gerekir.

1. A ----> B SYN, benim sıra numaram X'dir.
2. A <---- B ACK, senin sıra numaran X'dir.
3. A <---- B SYN, benim sıra numaram Y'dir.
4. A ----> B ACK, senin sıra numaran Y'dir.

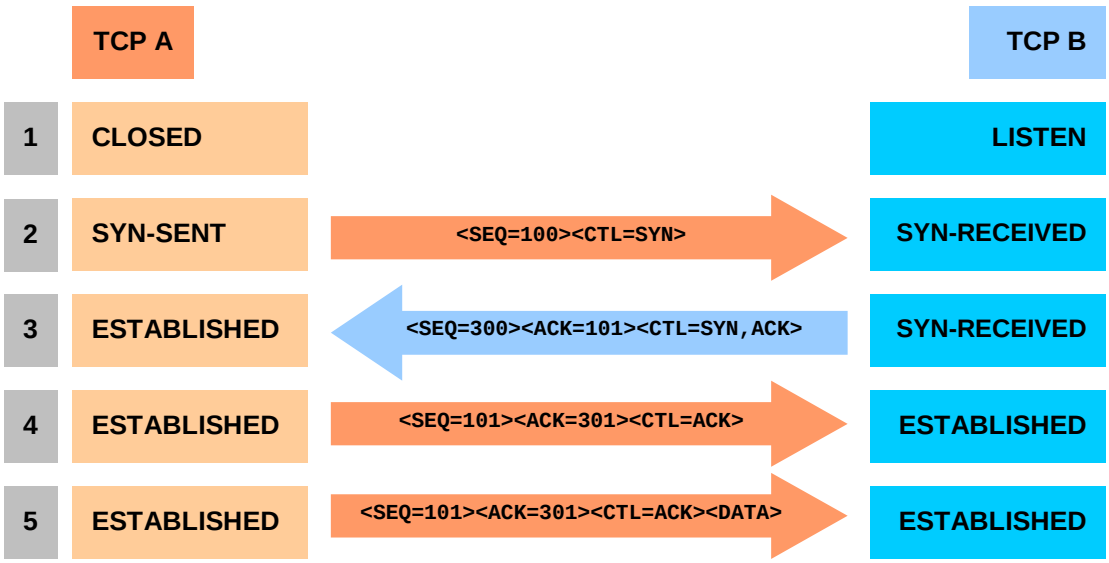
İkinci ve üçüncü adımlar tek bir mesaj içinde birleştirilebilir. Buna da "Üç Yollu El Sıkışma" denir.

Üç yollu el sıkışma bir bağlantı için gerçekten gereklidir. Çünkü, paket sıra numaraları ağ üzerinde global tanımlı değildir ve TCP'ler ISN seçiminde farklı mekanizmalar kullanabilir. Alıcı TCP'nin gelen numaranın daha önce gönderilmiş fakat gelmesi gecikmiş bir numara olup olmadığını anlayabilme gibi bir şansı yoktur. Bu yüzden ilk SYN numarasını göndericiye onaylatmak zorundadır.

1.3.1.7.5. Bağlantı Kurulumu ve Bağlantı Sorunlarının Giderilmesi

TCP daha önceden açık kalmış, bazı aksaklıklardan dolayı kopmuş ama karşı taraf için halen açık görülen bağlantılar ağ üzerinde karşıya ulaşmamış ve iletişim esnasında karşıya ulaşabilecek ve veri sırasını bozabilecek paketleri önlemek için sistemler arasında bağlantı kurarken üç yollu el sıkışma metodunu kullanır.

Bu metodun basitleştirilmiş gösterimi ve iletilen segment içerikleri şekil 6'da gösterilmiştir.

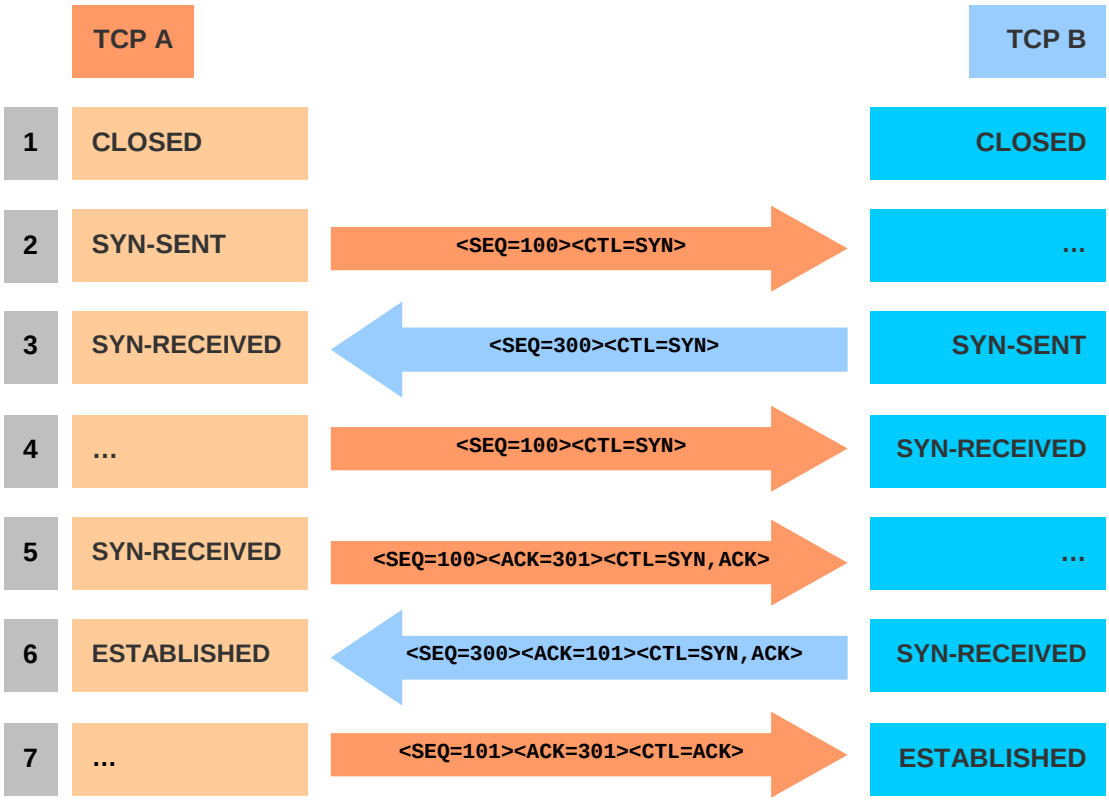


Şekil 6: Bağlantı senkronizasyonu için basitleştirilmiş üç yollu el sıkışma modeli

Şekli 6 incelersek ikinci satırda, TCP A kullanacağı sıra numaralarının <100> ile başlayacağını gösteren SYN segmenti göndererek başlıyor. Üçüncü satırda, TCP B bir SYN gönderiyor ve TCP A'dan aldığı SYN'yi onaylıyor. Burada dikkat edilmesi gereken bir nokta var. TCP B 100 sıra numaralı segmenti onaylamak için gönderdiği paketin onay alanında TCP A'nın bundan sonra göndermesi gereken sıra numarasının 101 olacağını bildiriyor.

Dördüncü satırda TCP A, TCP B'nin gönderdiği SYN mesajına karşılık ACK içeren boş bir segment gönderiyor ve beşinci satırda, TCP A ileteceği verinin bir kısmını gönderiyor. Dikkat edin; beşinci satırda kullanılan sıra numarası dördüncü satırdaki ile aynı. Çünkü dördüncü satırdaki ACK bir sıra numarası içermiyor. Yalnızca TCP B'nin 300 sıra numaralı mesajını aldığını ve TCP B'nin bir sonraki mesajının sıra numarasının 301 olacağını gösteriyor.

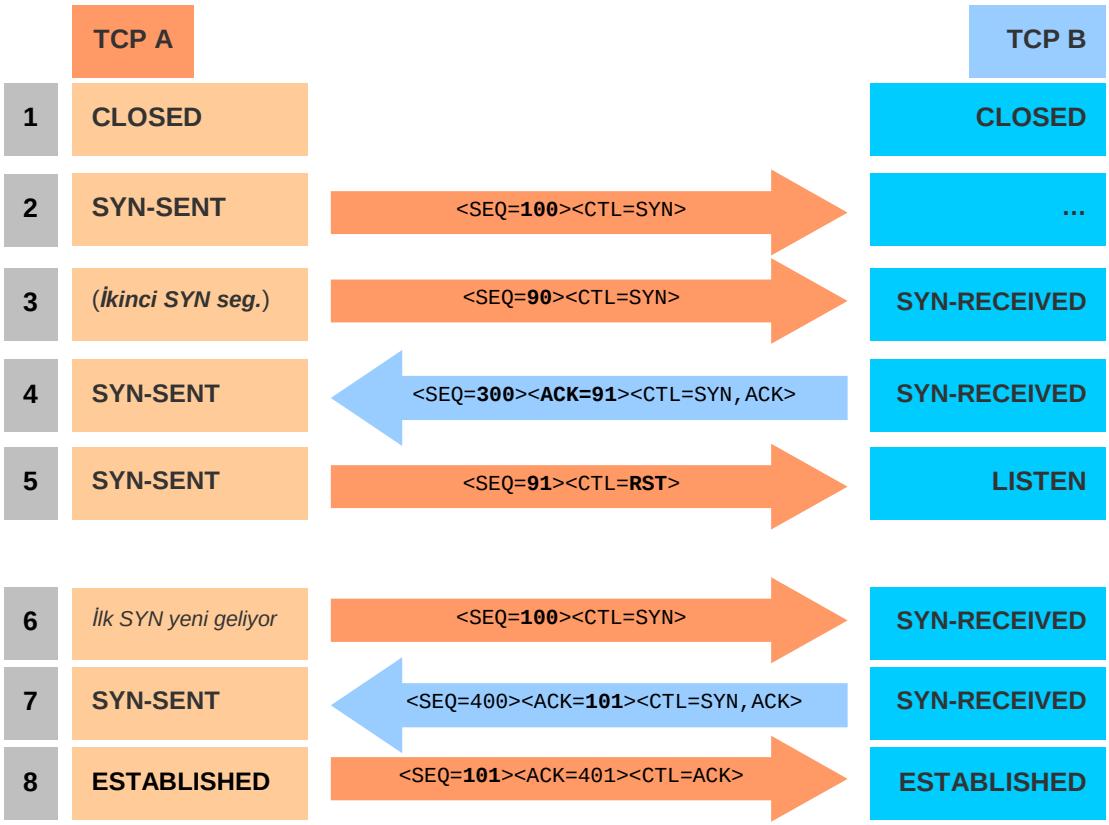
Aslında eş zamanlı anlaşmada bağlantı için yalnızca TCP A mesaj göndermez. Aynı anda TCP B de gönderir. Her bir TCP'nin CLOSED durumundan başlayıp karşılıklı olarak SYN-SENT, SYN-RECEIVED ve ESTABLISHED durumları için birbirlerine gönderdikleri segmentlerle senkronizasyonu nasıl sağladıklarını adım adım görelim.



Şekil 7: Eş zamanlı bağlantı Senkronizasyonu

Üç yollu el sıkışmada temel hedef, ağ ortamında dolaşan eski bağlantılardan kalmış segmentlerin bağlantı karmaşasına neden olmasını önlemektir. Bunun üstesinden gelebilmek için özel bir kontrol mesajı; " RESET " konulmuştur. Eğer alıcı TCP senkronize edilmemiş bir durumla karşılaşırsa bunu karşı TCP'ye bildirir ve kabul edilebilir bir RESET işareti için LISTEN (Dinleme) konumuna geçer. RESET işaretini aldığı anda bağlantıyı keser ve yeni bağlantı için hazırlanır.

Şimdi de ağ ortamında dolaşan bir segmentin yol açabileceği karmaşanın nasıl önlendiğine ve sağlıklı bir bağlantının tekrar nasıl kurulduğuna bakalım.



Şekil 8: Çift SYN Karmaşıklığının Giderilmesi

Şekil 8'de eskiden kalma bir SYN paketinin oluşturduğu karmaşanın çözümü görülmektedir. Üçüncü satırda TCP B'ye eski bir SYN segmenti ulaşıyor. TCP B bunun eski bir segment olduğunu bilemez. Bu nedenle dördüncü satırda normal bir şekilde buna yanıt veriyor. TCP A gelen onayda onay alanının uyuşmadığını fark ediyor ve segmentin inandırıcı ve kabul edilebilir olması için gelen onay segmentinin SEQ alanındaki numarayı kullanarak RST (Reset) gönderiyor. Paketi alan TCP B' RST işaretini görüyor ve derhal LISTEN durumuna geçiyor. İlk adımda gönderilen orijinal SYN sonunda ulaşıyor ve altıncı adımdan itibaren sağlıklı bağlantı sağlanıyor.

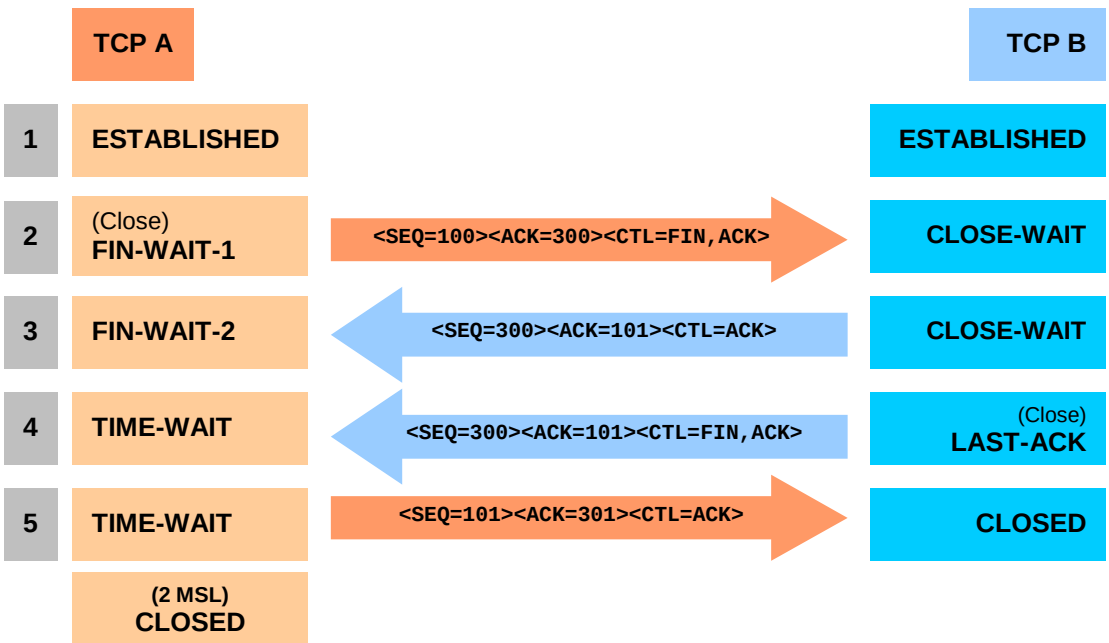
Aynı şekilde her iki TCP'de LISTEN durumundayken, ağ ortamında dolaşan varolmayan bir bağlantıya ait bir SYN alınabilir. Bu durumda SYN alan TCP B yine normal yanıt verir ve TCP A herhangi bir SYN göndermediği için bu segmentin ACK alanında bulunan numara ile RST işareti gönderir. Bunu alan TCP B bağlantıyı kesip LISTEN durumuna geçer.

Bütün RST işaretleri dikkate alınmaz. RST işaretini alan TCP'nin aldığı RST paketinin SEQ alanındaki numaranın kendisinin bir önce göndermiş olduğu ACK alanı ile uyması gerekir. Aksi halde gelen RST olsun yada başka bir segment olsun kabul etmez.

1.3.1.7.6. Bağlantının Sonlandırılması

Karşılıklı eş zamanlı el sıkışma mekanizmasıyla kurulan bağlantı yine karşılıklı eş zamanlı olarak kapatılıyor. TCP A transferin bittiğini gösterir FIN (FINish) segmenti gönderiyor. Bunu alan TCP B transferin bittiğini anlıyor ve FIN aldığını onaylayarak bir FIN de kendisi gönderiyor. Bunu alan TCP A aldığı FIN'i onaylıyor. Onayı alan TCP B bağlantıyı kapatıyor. TCP A ise iki MSL (Maximum Segment Lifetime – Azami Segment Ömrü) kadar bekleyip bağlantıyı sonlandırıyor.

Şimdi bu işlemin nasıl gerçekleştiğine şekil üzerinde bakalım.



Şekil 9: Eş zamanlı olarak karşılıklı bağlantı kapatma modeli

Her iki taraf da birbirlerine FIN segmenti göndererek onay aldıktan sonra bağlantıyı karşılıklı olarak sonlandırıyorlar.

1.3.1.8. Arayüzler

Kullanıcı/TCP ve TCP/Alt-Seviye olmak üzere iki TCP arayüzü vardır. Alt-Seviye arayüzü bildiğiniz üzere IP katmanını içerir. Burada TCP/Alt-Seviye arayüzünü değil, Kullanıcı/TCP arayüzünü inceleyeceğiz. Ayrıca Alt-Seviye arayüzünden TCP'nin ihtiyaç duyduğu birkaç terim de kullanılacaktır.

1.3.1.8.1. Kullanıcı/TCP arayüzü

Aşağıda bahsedeceğimiz kullanıcı komutları her işletim sisteminin farklı özelliklere sahip olması nedeniyle farklılık gösterebilir. Bu nedenle, farklı TCP uygulamalarının farklı

kullanıcı arayüzleri olacağını unutmayın. Bununla birlikte bütün TCP'lerde ortak noktadan iletişim kurmayı garanti edebilmesi için TCP uygulamalarının tamamı aynı protokol hiyerarşisini desteklemek zorundadır. Bu bölümde bütün TCP uygulamalarının ihtiyaç duyduğu fonksiyonel arayüzler anlatılacaktır.

1.3.1.8.2. TCP Kullanıcı Komutları

Burada kullanılan komut dizilimleri üst seviyeli dillerin prosedür ve fonksiyon çağrılarına benzemektedir. Aşağıda tanımlanan komutlar, TCP'nin süreçler arası iletişimi destekleyebilmesi çalıştırmak zorunda olduğu temel fonksiyonlardır.

TCP, süreçler arası iletişim kurarken sadece gelen komutları kabul etmez. Bunun yanında işlemin kendisinden istediği;

- Bağlantı hakkında genel bilgi (Örneğin, kesmeler, uzaktan kapatma, tanımlanmamış uzak soketleri bağlama gibi)
- Çeşitli hata tipleri veya başarı bildiren özel kullanıcı komutlarına yanıtlar,

gibi bilgileri geri vermek zorundadır.

OPEN Komutu

Kullanımı: OPEN (Yerel Port, Uzak Soket, Aktif/Pasif [, zamanaşımı] [, öncelik] [,güvenlik/bölme][, seçenekler] → Yerel Bağlantı Adı

Yerel TCP gelen işlemde verilen kimliği tanıyacak ve belirtilen bağlantıyı kullanmak için işlem yetkisini kontrol edecektir. TCP işlemine bağlı olarak, yerel ağ ve kaynak adres için TCP tanımlayıcıları karşı TCP veya alt-seviye protokolü (IP) tarafından sağlanacaktır. Bu prosedürler herhangi bir TCP'nin başkasıymış sahte bir TCP gibi davranmasını önlemek ve güvenliği sağlamak içindir.

Aktif/Pasif bayrağı eğer pasif ise bunun anlamı gelen bir bağlantı için LISTEN durumuna geç demektir. Tam tanımlı bir Pasif çağrı sonradan gelen bir SEND işlemi ile aktif hale getirilebilir.

TCB (İletim Kontrol Bloğu – Transmission Control Block)OPEN komutu parametreleri ile oluşturulur ve bir kısmı bu parametreler tarafından bazı bilgilerle doldurulur.

Aktif bir OPEN komutuyla TCP hemen bağlantının tek seferde senkronizasyonunun yapmak için prosedürlerini işletmeye başlar.

Zaman aşımı, eğer belirtilmişse karşı tarafın gönderdiği bütün verilere bir zaman aşımı koymasına izin verir. Eğer veri, belirtilen zaman aşımı süresince hedefe başarılı bir şekilde ulaşmamışsa TCP bağlantıyı koparacaktır. Varsayılan zaman aşım değeri beş dakikadır.

Öncelik ve Güvenlik/Bölüm, eğer belirtilmemişse varsayılan değerler kullanılacaktır. TCP, kendisine gelen istekleri sadece Güvenlik/Bölüm bilgisi kesinlikle aynı olan ve eğer Öncelikleri OPEN çağrısındaki ile eşit ya da yüksekse kabul eder. Aksi halde reddedecektir.

Yerel Bağlantı Adı, TCP tarafından kullanıcıya döndürülecektir. Yerel Bağlantı Adı daha sonra <Yerel Soket ve Uzak Soket> çifti ile tanımlanmış bağlantının yerine kullanılabilir.

SEND Komutu

Kullanımı: SEND (Yerel Bağlantı Adı, Önbellek Adresi, Bayt Sayısı, PUSH bayrağı, URGENT bayrağı [,Zaman Aşımı])

Bu fonksiyon çağrısı belirtilen kullanıcı önbelleğindeki bilginin belirtiler bağlantıya gönderilmesini sağlar. Eğer bağlantı açılmamışsa, SEND fonksiyonu hata verir.

PUSH bayrağı 1 ise veri alıcıya hemen iletilmelidir ve PUSH biti önbellekteki bilgilerden yaratılan son TCP segmentinde 1 yapılmalıdır. Eğer PUSH bayrağı işaretlenmemişse, veri etkin bir iletim olması amacıyla diğer verilerle birleştirilip gönderilmek üzere bekletilebilir.

URGENT (Acil) bayrağı etkin ise, hedefe gönderilen segmentlerde URG bayrağı etkindir. URGENT işaretçisinin amacı, bilinmeyen acil verinin tamamının alıcı tarafından alındığına dair alıcı üst katmanını uyarmaktır. Gönderici TCP'nin gönderdiği URGENT sinyalinin sayısının alıcının verinin acil olduğuna dair uyarılma sayısına eşit olmak zorunda değildir.

Eğer OPEN komutunda uzak soket belirtilmişse ama bağlantı onaylanmışsa (örneğin belirtilmeyen uzak soketlerde yerel soket LISTEN durumunda gelecek olan uzak bağlantı çağrılarını bekler. Bu şekilde bir bağlandı kurulmuş olabilir.) tanımlanmış önbellekten bilinmeyen uzak soket adresine SEND ile verileri gönderebilir.

Bununla birlikte, eğer SEND komutu uzak soket bağlantı istememiş ve tanımlanmamışken kullanılırsa hata verecektir. Kullanıcılar bağlantı durumunu kontrol etmek için STATUS fonksiyon çağrısını kullanabilirler. Bazı uygulamalarda TCP tanımlanmamış uzak bir soketten bağlantı olduğunda kullanıcıyı bilgilendirebilir.

Eğer bir Zaman Aşımı belirtilmişse, bu bağlantı için aktif kullanıcının zaman aşımı yenisiyle değiştirilir.

Basit bir uygulamayla, SEND fonksiyonu bütün iletim tamamlanana ya da zaman aşımı dolana kadar yeni bir gönderme işlemine geçmez. Bu basit metot her iki tarafın da herhangi bir RECEIVE işlemi olmadan sürekli SEND yapmalarıyla oluşabilecek hat kilitlenmelerini ve neden olabilecekleri hat kirliliğinden dolayı düşük performansa sebebiyet vermelerini önler.

RECEIVE Komutu

Kullanımı: RECEIVE (Yerel Bağlantı Adı, Önbellek Adresi, Bayt sayısı) → Bayt Sayısı, Urgent Bayrağı, Push Bayrağı

Bu komut, belirtilen bağlantıyla ilişkilendirilmiş alıcı önbelleğe verileri yerleştirir. Eğer OPEN komutu kullanılmamış veya çağrı yapan fonksiyon işlemi bu bağlantıyı kullanmaya yetkilendirilmemişse hata mesajı verir.

Daha kolay bir ifadeyle; Herhangi bir hata oluşana kadar yada önbellek dolana kadar işlem kontrolü çağrı yapan programa verilmez. Bu nedenle bu metot kilitlenmelerin öncelikli sebebi olmaktadır.

Eğer önbelleği dolduracak kadar veri gelmişse ve PUSH işareti görülmeden önbellek dolmuşsa, RECEIVE durumuna verilen yanıtta PUSH işaretçisi gönderilmez. Önbellek alabileceği bütün veriyi almadan dolmaz. Eğer önbellek dolmamışsa ve PUSH sinyali alınmışsa gönderilen onay sinyalinde PUSH bayrağı işaretlenir ve yeni veri alımına izin verilir.

Eğer URGENT (Acil) veri geliyorsa, veri ulaşır ulaşmaz TCP-to-user sinyali ile kullanıcı uyarılacaktır. Alıcı taraftaki kullanıcı "Acil Mod"a geçmiş olacaktır. Eğer URGENT bayrağı halen aktifse halen gelecek acil bilgiler var demektir. URGENT bayrağı pasifse bu çağrı RECEIVE komutunun bütün veriyi aldığını onayladığını bildirir. Şimdi kullanıcı artık "Acil Mod"dan çıkabilir. Acil verileri takip eden acil olmayan veriler acil önbelleğine iletilemezler. Çünkü acil verilerle acil olmayanların sınırları açık bir şekilde belirtilmiştir.

CLOSE komutu

Kullanımı: CLOSE (Yerel Bağlantı Adı)

Bu komut belirtilen bağlantının kapanmasına neden olur. Eğer bağlantı açık değilse veya çağrı yapan fonksiyon bu bağlantıyı kullanmaya yetkili değilse hata mesajı verir.

Her ne kadar bağlantı kapatılıyor olsa da bu arada veri alımına devam edilebilir. Çünkü karşı taraf verilerinin son parçalarını gönderiyor olabilir. Buna göre; CLOSE "Gönderecek Başka Verim Kalmadı anlamındadır. Kesinlikle "Bundan Sonra Veri Almıyorum" anlamına gelmez. Bu gibi durumlarda kapatan taraf karşıdan gelen bilgileri kesemez. Eğer zaman aşımı içinde bilgi gelmeye devam ederse CLOSE komutu ABORT'a (İptal) geçer ve kapatan taraftaki TCP kapatma işleminden vazgeçer.

Ayrıca kullanıcı istediği herhangi bir zamanda bağlantıyı kendi insiyatifiyle veya TCP'nin verdiği mesajlara göre kapatabilir (örneğin, uzak kapatma çağrısı, iletim zamanaşımı, hedefin ulaşılamaz olması gibi mesajlar).

Çünkü bir bağlantıyı kapatma işlemi uzak TCP'nin bilgisi dahilin de olması gerekir. Kapanma durumunda kısa bir süre için iletişim durumunda kalınabilir. Uzak TCP'nin

kapanma isteğine yanıt vermesinden önce bağlantıyı yeniden açma girişimleri hata verecektir.

STATUS Komutu

Kullanımı: STATUS (Yerel Bağlantı Adı) → Durum Bilgisi

Bu komut, kullanıcı komutlarına bağlı olarak gelen bir karşılıktır ve uzak TCP'de herhangi bir etki yapmaz. Yerel Bağlantıda belirtilen uzak TCP'den aldığı bağlantı durum bilgilerini getirir.

Bu komut:

- Yerel Soket,
- Uzak Soket,
- Yerel Bağlantı Adı,
- Alım Penceresi,
- Bağlantı Durumu,
- Onay Bekleyen Önbellek Sayısı,
- Rapor Gönderen Önbellek Sayısı,
- Urgent (Acil) Durumu,
- Öncelik,
- Güvenlik/Bölüm Bilgisi,
- Ve İletim Zaman Aşım Süresi;

bilgilerini içeren veri blokları getirir.

Bağlantı durumuna göre veya kendi uygulamalarına göre bu bilgilerin bazıları alınamayabilir veya anlamız olabilir. Eğer çağrı yapan fonksiyon bu bağlantıyı kullanma yetkisine sahip değilse hata bilgisi geriye döner. Bu metot bağlantı hakkında izinsiz uygulamaların bilgi toplamasına engel olur.

ABORT Komutu

Kullanımı: ABORT (Yerel Bağlantı Adı)

Bu komut bekleyen bütün gönderim ve alımları durdurur, TCB (İletim Kontrol Bloğu– Transmission Control Block) bloklarını siler ve bağlantının diğer ucundaki TCP'ye özel bir RESET mesajı gönderir. Uygulamaya bağlı olarak; kullanıcılar beklemede olan gönderim ve alımlardan ABORT bildirimi alabilir veya bir ABORT onay bildiririmi alabilir.

TCP'den Kullanıcıya Mesajlar

İşletim sistemi çevresel birimleri kullanıcı programa iletmek için TCP'den eş zamanlı olmayan sinyaller ister. TCP kullanıcı programa sinyal iletirken kesin bilgiler verir. Bu

bilgiler; SEND ya da RECEIVE veya diğer kullanıcı çağrılarının tamamlanmasına dair aşağıdaki bilgilerdir.

Yerel Bağlantı Adı	Her zaman
Yanıt String Dizisi	Her zaman
Önbellek Adresleri	Gönderim & Alım
Bayt Sayısı (Gelen Paketleri Sayar)	Alım
Push Bayrağı	Alım
Urgent Bayrağı	Alım

Sonuç olarak TCP taşıma katmanında bilgiler paketlere bölünerek iletildiğini gördük. Bu paketlerin her birine segment denildiğini artık biliyoruz. Bilgileri karşıdaki diğer bilgisayardaki TCP'ye gönderebilmek için gönderen taraf ile alıcı taraf arasında bağlantı kurmak gerekir. İnternet'i düşünün. Birbirine bağlı milyonlarca bilgisayardan hangisine bilgi göndereceğinizi bilemezdiniz. Bu yüzden iki bilgisayar karşılıklı anlaşarak aralarında mantıksal bir bağlantı kuruyorlar. Aralarında birbirlerine gönderecekleri her türlü pakete verecekleri numaraların kaçtan başlayacağı konusunda anlaşıyorlar. Araya eskiden kalma bir paket girerse, başka bir bilgisayardan sızma olacak olursa veya hatta problemler olur da bağlantıda aksaklıklar olursa hemen bağlantıyı yeniliyorlar. Böylece iki bilgisayar güvenli bir şekilde iletişim kurup veri iletimi yapıyorlar.

Bu iletim sisteminde bilgi gönderen tarafa sunucu, bilgi alan tarafa da istemci diyoruz. Sunucu ve istemci arasındaki bilgiler nihayetinde fiziksel katmanda 1 ve 0'a karşılık gelen elektriksel sinyallerle iletiliyor. Sunucu ve istemcide kurulan soketler her iki tarafta da hem sunucu hem de istemci olarak görev yapabiliyor. Aşağıdaki tabloda her iki tarafında bağlantıda hangi işlemleri yaptığını görebiliriz.

İstemci	Sunucu
Soket oluştur, **`socket()`**	Soket Oluştur, **`socket()`**
	Adres bilgilerini yerleştir, **`sockaddr_in`**
	Soket adını adresiyle ilişkilendir, **`bind()`**
	Soketi dinlemeye geç, **`bind()`**
Bağlantı yap, **`connect()`**	Bağlantıyı kabul et, **`accept()`**
Veri gönder, **`send()`**	Veri al, **`recv()`**
Veri al, **`recv()`**	Veri gönder, **`send()`**
… Diğer işlemler… …	… Diğer işlemler… …
Soketi kapat, **`close()`**	Soketi kapat, **`close()`**

Tablo 6: TCP sunucu ve istemci soket uygulamaları.

Bu bağlantılı, kontrollü ve güvenli işlemi TCP sağlıyor.

1.3.2. UDP

UDP (User Datagram Protocol – Kullanıcı Datagram Protokolü) TCP ile birlikte aynı taşıma katmanında bulunan, kararlı bir iletim gerektirmeyen uygulamalar için geliştirilmiş basit bir iletim protokolüdür.

Birbirine bağlı bilgisayarların oluşturduğu bir ağ içerisinde paket anahtarlamalı bilgisayar iletişiminin datagram modunu kullanılabilir hale getirmek için tanımlanmıştır. TCP gibi bağlantılı, güvenli, garantili bir iletim yapmaz. Aklınıza bu soru gelebilir. UDP güvenli değil, neden kullanılıyor?

UDP, TCP'den daha hızlı çalışıyor ve daha hızlı iletim yapıyor. TCP her veri paketini gönderdikten sonra alıcıdan onay bekler, paket hatalı iletilmiş mi, bağlantı zayıflamış mı, alıcı doğru paketi mi almış, araya başka bağlantılar mı girmiş, karşı tarafın alabileceğinden daha fazla mı veri gönderilmiş, onay gelmemiş paketleri belirlendi mi, onlar tekrar gönderildi mi gibi birçok olasılığı sürekli kontrol eder. Bu olasılıkların her biri gerçekleştiği anda ayrı ayrı çözümleniyor ve veri iletimi kesinlikle tam olarak gerçekleştirilmiş oluyor.

Buraya kadar her şey güzel de, bizim göndereceğimiz verilerin arada kayıplara uğraması çok da önemli değilse ve hızlı bir şekilde iletilmesini istiyorsak TCP bizi yavaşlatacaktır. Örneğin İnternet üzerinde ses iletimi, görüntü iletimi, bunlar hızlı iletilmesi gereken bilgilerdir. Arada birkaç paket kayba uğrasa seyreden bunu fark edemez. Ya da bir karelerin birkaçının sırası karışsa, saniyede geçen 25 karenin arasında bunu kim fark edebilir?

Bu kontroller yüzünden görüntünün kare kare gelmesini, duraklamasını kimse istemez. İşte bu noktada UDP devreye giriyor ve bu kontrollerin hiçbirini yapmaz. İki bilgisayar arasında bir bağlantı kurulduğu anda karşı bilgisayarın paketleri başarılı bir şekilde aldığını varsayarak sürekli bir gönderim yapar. Göndereceği veri bittikten sonra da bağlantıyı kapatır. Böylece bizim görüntü bilgileri kontrollere uğramadan, hızlı bir şekilde iletilmiş olur. Biz de arada birkaç kare kaybı fark bile etmeyiz. Şimdi UDP'yi biraz tanıyalım.

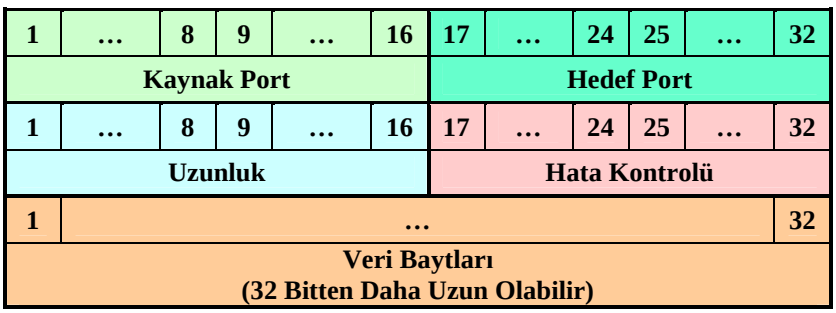
UDP protokolü üst katmanında bulunan uygulama programlarına, minimum protokol mekanizması kullanarak hedef bilgisayarda bulunan diğer uygulama programlarına mesaj gönderebilmeleri için bir prosedür sağlar. TCP bağlantı merkezlidir (connection oriented), bağlantının sağlamlığı önceliklidir, UDP ise işlem merkezlidir (transaction oriented), öncelik veri iletme işlemindedir**.** UDP rastgele iletim yapmaz. Hata kontrolü yapar fakat TCP kadar detaylı değildir. TCP'nin verdiği ulaştırma ve mükerrer iletim yapmama garantisi vermez. Bu yüzden sıralı bir şekilde güvenli ve güvenilir bir iletim gerektiren uygulamalar UDP değil TCP kullanırlar.

1.3.2.1. UDP Başlığı

TCP gibi UDP de verileri paketlere bölerek iletim yapar. Bu paketlere TCP'de segment, UDP'de ise datagram denir. UDP'nin datagram şekli TCP'nin paketlerine

benzerdir. Fakat daha basit bir yapısı vardır. Sıra numarası alanı, onay alanı, kontrol bölümleri, veri ofset alanı, bayraklar, alım penceresi alanı, acil işaretçi alanı, seçenek alanı, doldurma bitleri çıkartılmıştır. Çünkü UDP bu kontrolleri yapmaz. Kullanıcıyı bu kontrol yükünden kurtarır, sade yapıdaki datagramları hızlı bir şekilde iletir.

Gönderim yaparken, UDP üstteki uygulama katmanından gelen verileri alır, iletime rehberlik etmek için port numaralarını ekler, alıcı tarafta kullanılmak üzere hata kontrol alanına koyacağı bilgiyi hesaplar ve bunların hepsini birleştirip IP katmanına gönderir. Alım yaparken de bu işlemlerin tersini yapar.



Şekil 10: UDP başlığı alanları

1.3.2.1.1 Alanlar

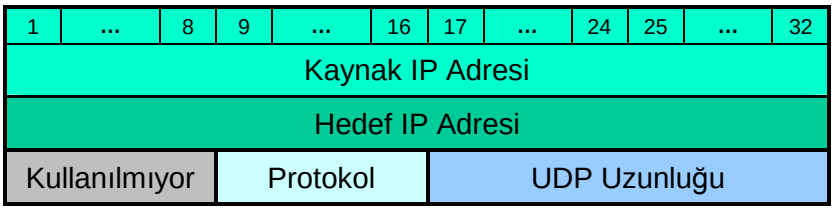
Kaynak Port: Opsiyonel bir alandır, bir bilgi kaybı durumunda ya da başka bir bilgi iletileceğinde mesaj gönderilecek adresin neresi olduğunu, yani göndericinin port numarasını belirtir. Eğer gönderici portu belirtilmezde bu alan “0” bilgisiyle doldurulur.

Hedef Port: Bir hedef İnternet adresiyle birlikte anlam kazanan port numarasıdır. Bilgi paketlerinin iletileceği hedef adresi belirtir.

Uzunluk: Başlık ve veri alanları dahil UDP paketinin tamamının uzunluğunu belirtir. Bu durumda veri olmasa bile başlık alanları nedeniyle paketin minimum uzunluğu 8 bayt olacaktır.

Hata Kontrolü: IP başlığı bilgileri ile mantıksal başlığın toplamının 16 bitlik birlere göre tümleyenidir. Bu alanda, UDP başlığı ve veri sonu, (gerekli ise) iki bayta tamamlamak için “0” ile doldurularak karşı tarafa gönderilir. Alıcı kendisine gelen bu 16 bitlik alanı alarak tümleyen aritmetiğinde çözümler. Sonuçta bütün bitler “1” ise hatasız iletilmiştir. Eğer herhangi bir “0” görülürse, hata olduğu anlaşılır. Bu durumda alınan datagram atılır.

Mantıksal başlık kaynak adresi, hedef adresi, kullanılan protokolü ve UDP uzunluğunu içeren, kavramsal olarak UDP başlığının önüne eklenmiş bir bilgidir. Bu bilgi yanlış yönlendirilebilecek paketlere karşı bir koruma sağlar. Bu hata kontrol prosedürünün kullanımı TCP ile aynıdır.



Şekil 11: Mantıksal başlık yapısı.

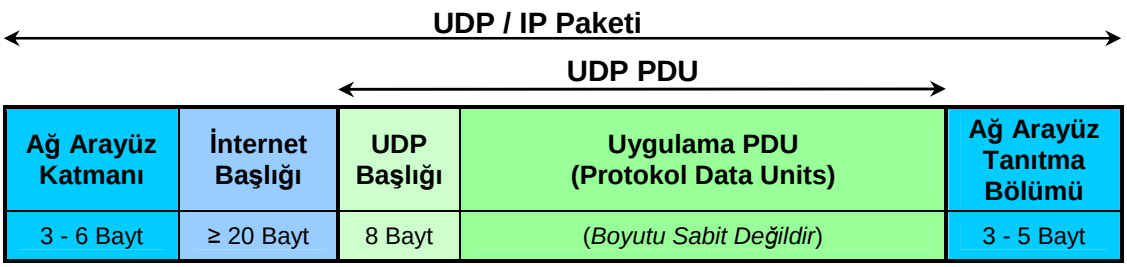
Eğer işlenen hata kontrolü "0" ise, iletilen bilginin tamamı "1"dir (tümler aritmetiğine göre 1'in tümleyeni 0'dır). Fakat iletilen bütün "0" hata kontrol değerleri, göndericinin herhangi bir hata kontrol değeri üretmediği anlamına gelir.

1.3.2.2. Kullanıcı Arayüzü

Bir UDP kullanıcı arayüzü,

- Yeni alım portları oluşturmaya,
- Alım portlarında, geri dönen veri baytları ile kaynak port ve adres işareti alım işlemlerine,
- Bir datagramın, gönderimine, veri tanımlamasına, gönderilecek kaynak ve hedef port ve adres işlemlerine izin veren bir uygulamaya olanak sağlamalıdır.

1.3.2.3. IP arayüzü



Şekil 12: UDP / IP paket alanları

Bir UDP modülü, İnternet başlığındaki kaynak ve hedef İnternet adreslerini ve protokol alanını saptayabilmelidir. Muhtemel bir UDP/IP arayüzü alım işleminde verilen dönütlerin İnternet başlıklarının hepsi dahil bütün İnternet Datagramını işler. Bir arayüz aynı zamanda UDP'nin İnternet Datagramının tamamını başlığı ile birlikte gönderilmesi için IP'ye teslim etmesine olanak tanır. IP tutarlılığı sağlamak ve Internet Başlığında hata kontrol alanını hesaplamak için Datagram başlıklarındaki belirli alanları kontrol eder.

Port	*Açıklama*
53	Domain Name System
67	Dynamic Host Configuration Protocol (DHCP) Client
68	Dynamic Host Configuration Protocol (DHCP) Server
69	Trivial File Transfer Protocol (TFTP)
137	NetBIOS Name Service
138	NetBIOS Datagram Service
161	SNMP Simple Network Management Protocol

Tablo 5: İyi Bilinen UDP Portları

UDP datagramları, istekler, cevaplar, defalarca tekrarlanan duyurular, kısa mesajlar için ideal bir taşıma protokolüdür. Buna ek olarak, IP çoklu yayın veya genel yayın adreslerine doğru yapılan çoklu yöne gönderilen veriler için de çok az iç kontrol mekanizması kullanmasından dolayı yaygın olarak kullanılır.

1.3.3. TCP VE UDP Port Numaraları

Bilgisayarda ağ üzerinde yapılan iletişimler port adı verilen kapılar üzerinden yapılır. Her protokol farklı kapılar kullanır. Bu kapılardan bazıları belirli programlara ve protokollere tahsis edilmiştir. Kullandığımız TCP ve UDP protokollerine ayrılan portlar aşağıda listelenmiştir.

UYARI → Sevgili öğrenci; aşağıda verilmiş TCP ve UDP protokollerine ayrılan portlar listesini ezberlemenize gerek yoktur. Gerektiğinde bakmanız yeterlidir.

Port	Protokol	Anahtar Sözcük	Açıklama
0	tcp, udp	Reserved	
1	tcp, udp	tcpmux	TCP Port Service Multiplexer
2	tcp, udp	compressnet	Management Utility
3	tcp, udp	compressnet	Compression Process
4	tcp, udp	Unassigned	
5	tcp, udp	RJE	Remote Job Entry
6	tcp, udp	Unassigned	

7	tcp, udp	echo	Echo
8	tcp, udp	Unassigned	
9	tcp, udp	discard	Discard; alias=sink null
10	tcp, udp	Unassigned	
11	udp	systat	Active Users; alias=users
12	tcp, udp	Unassigned	
13	tcp, udp	daytime	Daytime
14	tcp, udp	Unassigned	
15	tcp, udp	Unassigned	[was netstat]
16	tcp, udp	Unassigned	
17	tcp, udp	qotd	Quote of the Day; alias=quote
18	tcp, udp	msp	Message Send Protocol
19	tcp, udp	chargen	Character Generator; alias=ttytst source
20	tcp, udp	ftp-data	File Transfer [Default Data]
21	tcp, udp	ftp	File Transfer [Control], connection dialog
22	tcp, udp	Unassigned	
23	tcp, udp	telnet	Telnet
24	tcp, udp	Any private	mail system
25	tcp, udp	smtp	Simple Mail Transfer; alias=mail
26	tcp, udp	Unassigned	
27	tcp, udp	nsw-fe	NSW User System FE
28	tcp, udp	Unassigned	
29	tcp, udp	msg-icp	MSG ICP
30	tcp, udp	Unassigned	
31	tcp, udp	msg-auth	MSG Authentication
32	tcp, udp	Unassigned	
33	tcp, udp	DSP	Display Support Protocol
34	tcp, udp	Unassigned	
35	tcp, udp	Any private	printer server
36	tcp, udp	Unassigned	
37	tcp, udp	time	Time; alias=timeserver
38	tcp, udp	Unassigned	
39	tcp, udp	rlp	Resource Location Protocol; alias=resource
40	tcp, udp	Unassigned	
41	tcp, udp	graphics	Graphics
42	tcp, udp	nameserver	Host Name Server; alias=nameserver
43	tcp, udp	nicname	Who Is; alias=nicname
44	tcp, udp	mpm-flags	MPM FLAGS Protocol
45	tcp, udp	mpm	Message Processing Module
46	tcp, udp	mpm-snd	MPM [default send]
47	tcp, udp	ni-ftp	NI FTP
48	tcp, udp	Unassigned	
49	tcp, udp	login	Login Host Protocol
50	tcp, udp	re-mail-ck	Remote Mail Checking Protocol
51	tcp, udp	la-maint	IMP Logical Address Maintenance
52	tcp, udp	xns-time	XNS Time Protocol
53	tcp, udp	domain	Domain Name Server

54	tcp, udp	xns-ch	XNS Clearinghouse
55	tcp, udp	isi-gl	ISI Graphics Language
56	tcp, udp	xns-auth	XNS Authentication
57	tcp, udp	Any	private terminal access
58	tcp, udp	xns-mail	XNS Mail
59	tcp, udp	Any private	file service
60	tcp, udp	Unassigned	
61	tcp, udp	ni-mail	NI MAIL
62	tcp, udp	acas	ACA Services
63	tcp, udp	via-ftp	VIA Systems - FTP
64	tcp, udp	covia	Communications Integrator (CI)
65	tcp, udp	tacacs-ds	TACACS-Database Service
66	tcp, udp	sql*net	Oracle SQL*NET
67	tcp, udp	bootpc	DHCP/BOOTP Protocol Server
68	tcp, udp	bootpc	DHCP/BOOTP Protocol Server
69	udp	TFTP	Trivial File Transfer Protocol
70	tcp, udp	gopher	Gopher
71	tcp, udp	netrjs-1	Remote Job Service
72	tcp, udp	netrjs-2	Remote Job Service
73	tcp, udp	netrjs-3	Remote Job Service
74	tcp, udp	netrjs-4	Remote Job Service
75	udp	Any private	dial out service
76	tcp, udp	Unassigned	
77	tcp, udp	Any private	RJE service
78	tcp, udp	vettcp	Vettcp
79	tcp, udp	finger	Finger
80	tcp, udp	www	World Wide Web HTTP
81	tcp, udp	hosts2-ns	HOSTS2 Name Server
82	tcp, udp	xfer	XFER Utility
83	tcp, udp	mit-ml-dev	MIT ML Device
84	tcp, udp	ctf	Common Trace Facility
85	tcp, udp	mit-ml-dev	MIT ML Device
86	tcp, udp	mfcobol	Micro Focus Cobol
87	tcp, udp	Any private	terminal link; alias=ttylink
88	tcp, udp	kerberos	Kerberos
89	tcp	su-mit-tg	SU MIT Telnet Gateway
89	udp	su-mit-tg	SU MIT Telnet Gateway
90	tcp, udp	DNSIX	Security Attribute Token Map
91	tcp, udp	mit-dov	MIT Dover Spooler
92	tcp, udp	npp	Network Printing Protocol
93	tcp, udp	dcp	Device Control Protocol
94	tcp, udp	objcall	Tivoli Object Dispatcher
95	tcp, udp	supdup	SUPDUP
96	tcp, udp	dixie	DIXIE Protocol Specification
97	tcp, udp	swift-rvf	Swift Remote Virtual File Protocol
98	tcp, udp	tacnews	TAC News
99	tcp, udp	metagram	Metagram Relay

100	tcp	newacct	[unauthorized use]
101	tcp, udp	hostname	NIC Host Name Server; alias=hostname
102	tcp, udp	iso-tsap	ISO-TSAP
103	tcp, udp	gppitnp	Genesis Point-to-Point Trans Net; alias=webster
104	tcp, udp	acr-nema	ACR-NEMA Digital Imag. & Comm. 300
105	tcp, udp	csnet-ns	Mailbox Name Nameserver
106	tcp, udp	3com-tsmux	3COM-TSMUX
107	tcp, udp	rtelnet	Remote Telnet Service
108	tcp, udp	snagas	SNA Gateway Access Server
109	tcp, udp	pop2	Post Office Protocol - Version 2; alias=postoffice
110	tcp, udp	pop3	Post Office Protocol - Version 3; alias=postoffice
111	tcp, udp	sunrpc	SUN Remote Procedure Call
112	tcp, udp	mcidas	McIDAS Data Transmission Protocol
113	tcp, udp	auth	Authentication Service; alias=authentication
114	tcp, udp	audionews	Audio News Multicast
115	tcp, udp	sftp	Simple File Transfer Protocol
116	tcp, udp	ansanotify	ANSA REX Notify
117	tcp, udp	uucp-path	UUCP Path Service
118	tcp, udp	sqlserv	SQL Services
119	tcp, udp	nntp	Network News Transfer Protocol; alias=usenet
120	tcp, udp	cfdptkt	CFDPTKT
121	tcp, udp	erpc	Encore Expedited Remote Pro.Call
122	tcp, udp	smakynet	SMAKYNET
123	tcp, udp	ntp	Network Time Protocol; alias=ntpd ntp
124	tcp, udp	ansatrader	ANSA REX Trader
125	tcp, udp	locus-map	Locus PC-Interface Net Map Server
126	tcp, udp	unitary	Unisys Unitary Login
127	tcp, udp	locus-con	Locus PC-Interface Conn Server
128	tcp, udp	gss-xlicen	GSS X License Verification
129	tcp, udp	pwdgen	Password Generator Protocol
130	tcp, udp	cisco-fna	Cisco FNATIVE
131	tcp, udp	cisco-tna	Cisco TNATIVE
132	tcp, udp	cisco-sys	Cisco SYSMAINT
133	tcp, udp	statsrv	Statistics Service
134	tcp, udp	ingres-net	INGRES-NET Service
135	tcp, udp	loc-srv	Location Service
136	tcp, udp	profile	PROFILE Naming System
137	tcp, udp	netbios-ns	NetBIOS Name Service
138	tcp, udp	netbios-dgm	NetBIOS Datagram Service
139	tcp, udp	netbios-ssn	NetBIOS Session Service
140	tcp, udp	emfis-data	EMFIS Data Service
141	tcp, udp	emfis-cntl	EMFIS Control Service
142	tcp, udp	bl-idm	Britton-Lee IDM
143	tcp, udp	imap2	Interim Mail Access Protocol v2
144	tcp, udp	news	NewS; alias=news
145	tcp, udp	uaac	UAAC Protocol
146	tcp, udp	iso-ip0	ISO-IP0

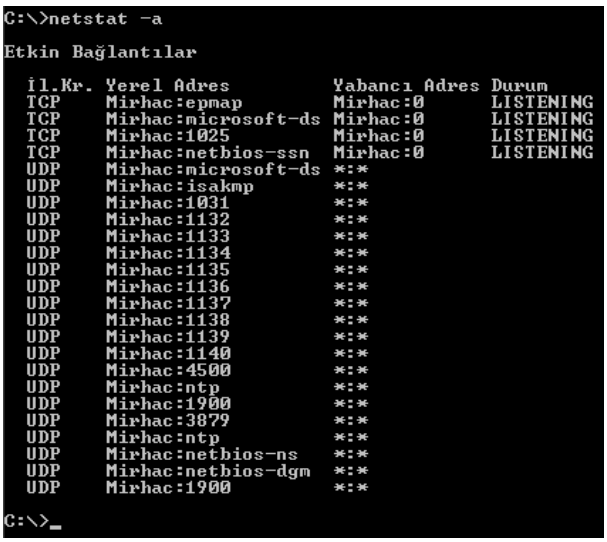
147	tcp, udp	iso-ip	ISO-IP
148	tcp, udp	cronus	CRONUS-SUPPORT
149	tcp, udp	aed-512	AED 512 Emulation Service
150	tcp, udp	sql-net	SQL-NET
151	tcp, udp	hems	HEMS
152	tcp, udp	bftp	Background File Transfer Program
153	tcp, udp	sgmp	SGMP; alias=sgmp
154	tcp, udp	netsc-prod	Netscape
155	tcp, udp	netsc-dev	Netscape
156	tcp, udp	sqlsrv	SQL Service
157	tcp, udp	knet-cmp	KNET/VM Command/Message Protocol
158	tcp, udp	pcmail-srv	PCMail Server; alias=repository
159	tcp, udp	nss-routing	NSS-Routing
160	tcp, udp	sgmp-traps	SGMP-TRAPS
161	tcp, udp	snmp	SNMP; alias=snmp
162	tcp, udp	snmptrap	SNMPTRAP
163	tcp, udp	cmip-man	CMIP/TCP Manager
164	tcp, udp	cmip-agent	CMIP/TCP Agent
165	tcp, udp	xns-courier	Xerox
166	tcp, udp	s-net	Sirius Systems
167	tcp, udp	namp	NAMP
168	tcp, udp	rsvd	RSVD
169	tcp, udp	send	SEND
170	tcp, udp	print-srv	Network PostScript
171	tcp, udp	multiplex	Network Innovations Multiplex
172	tcp, udp	cl/1	Network Innovations CL/1
173	tcp, udp	xyplex-mux	Xyplex
174	tcp, udp	mailq	MAILQ
175	tcp, udp	vmnet	VMNET
176	tcp, udp	genrad-mux	GENRAD-MUX
177	tcp, udp	xdmcp	X Display Manager Control Protocol
178	tcp, udp	nextstep	NextStep Window Server
179	tcp, udp	bgp	Border Gateway Protocol
180	tcp, udp	ris	Intergraph
181	tcp, udp	unify	Unify
182	tcp, udp	audit	Unisys Audit SITP
183	tcp, udp	ocbinder	OCBinder
184	tcp, udp	ocserver	OCServer
185	tcp, udp	remote-kis	Remote-KIS
186	tcp, udp	kis	KIS Protocol
187	tcp, udp	aci	Application Communication Interface
188	tcp, udp	mumps	Plus Five's MUMPS
189	tcp, udp	qft	Queued File Transport
190	tcp, udp	gacp	Gateway Access Control Protocol
191	tcp, udp	prospero	Prospero
192	tcp, udp	osu-nms	OSU Network Monitoring System
193	tcp, udp	srmp	Spider Remote Monitoring Protocol

194	tcp, udp	irc	Internet Relay Chat Protocol
195	tcp, udp	dn6-nlm-aud	DNSIX Network Level Module Audit
196	tcp, udp	dn6-smm-red	DNSIX Session Mgt Module Audit Redir
197	tcp, udp	dls	Directory Location Service
198	tcp, udp	dls-mon	Directory Location Service Monitor
199	tcp, udp	smux	SMUX
200	tcp, udp	src	IBM System Resource Controller
201	tcp, udp	at-rtmp	AppleTalk Routing Maintenance
202	tcp, udp	at-nbp	AppleTalk Name Binding
203	tcp, udp	at-3	AppleTalk Unused
204	tcp, udp	at-echo	AppleTalk Echo
205	tcp, udp	at-5	AppleTalk Unused
206	tcp, udp	at-zis	AppleTalk Zone Information
207	tcp, udp	at-7	AppleTalk Unused
208	tcp, udp	at-8	AppleTalk Unused
209	tcp, udp	tam	Trivial Authenticated Mail Protocol
210	tcp, udp	z39.50	ANSI Z39.50
211	tcp, udp	914c/g	Texas Instruments 914C/G Terminal
212	tcp, udp	anet	ATEXSSTR
213	tcp, udp	ipx	IPX
214	tcp, udp	vmpwscs	VM PWSCS
215	tcp, udp	softpc	Insignia Solutions
216	tcp, udp	atls	Access Technology License Server
217	tcp, udp	dbase	dBASE UNIX
218	tcp, udp	mpp	Netix Message Posting Protocol
219	tcp, udp	uarps	Unisys ARPs
220	tcp, udp	imap3	Interactive Mail Access Protocol v3
221	tcp, udp	fln-spx	Berkeley rlogind with SPX auth
222	tcp, udp	fsh-spx	Berkeley rshd with SPX auth
223	tcp, udp	cdc	Certificate Distribution Center
224-241			Reserved
243	tcp, udp	sur-meas	Survey Measurement
245	tcp, udp	link	LINK
246	tcp, udp	dsp3270	Display Systems Protocol
247-255			Reserved
345	tcp, udp	pawserv	Perf Analysis Workbench
346	tcp, udp	zserv	Zebra server
347	tcp, udp	fatserv	Fatmen Server
371	tcp, udp	clearcase	Clearcase
372	tcp, udp	ulistserv	UNIX Listserv
373	tcp, udp	legent-1	Legent Corporation
374	tcp, udp	legent-2	Legent Corporation
512	tcp	print	Windows NT Server için LDP
519	tcp, udp	utime	Unixtime
520	tcp	efs	Extended file name server
520	udp	router	Local routing process (on site); uses variant of Xerox NS routing information protocol;alias=router routed

525	tcp, udp	timed	Timeserver
526	tcp, udp	tempo	Newdate
530	tcp, udp	courier	RPC
531	tcp	conference	Chat
531	udp	rvd-control	MIT disk
532	tcp, udp	netnews	Readnews
533	tcp, udp	netwall	For emergency broadcasts
540	tcp, udp	uucp	Uucpd
544	tcp, udp	kshell	Krcmd; alias=cmd
550	tcp, udp	new-rwho	New-who
556	tcp, udp	remotefs	Rfs server; alias=rfs_server rfs
560	tcp, udp	rmonitor	Rmonitord
562	tcp, udp	chshell	Chcmd
564	tcp, udp	9pfs	Plan 9 file service
565	tcp, udp	whoami	Whoami
570	tcp, udp	meter	Demon
571	tcp, udp	meter	Udemon
600	tcp, udp	ipcserver	Sun IPC server
607	tcp, udp	nqs	Nqs
740	tcp, udp	netcp	NETscout Control Protocol
741	tcp, udp	netgw	NetGW
742	tcp, udp	netrcs	Network based Rev. Cont. Sys.
744	tcp, udp	flexlm	Flexible License Manager
747	tcp, udp	fujitsu-dev	Fujitsu Device Control
748	tcp, udp	ris-cm	Russell Info Sci Calendar Manager
749	tcp, udp	kerberos-adm	Kerberos administration
750	tcp	rfile	Kerberos authentication; alias=kdc
751	tcp, udp	pump	Kerberos authentication
752	tcp, udp	qrh	Kerberos password server
753	tcp, udp	rrh	Kerberos userreg server
754	tcp, udp	tell	Send; Kerberos slave propagation

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Bilgisayar laboratuarınızda ağ kablolarının nerelere takılı olduğunu tesbit edin.	➢ Ağ kablolarının takıldığı her cihazın iletişim için üzerinden geçersiniz.
➢ Ağ elemanlarının elektrik fişlerinin takılmış, çalışır durumda olduğundan ve bilgisayarınızın ağ bağlantısının var olduğundan emin olun.	➢ Genellikle bir ucu bilgisayarınıza, diğer ucu ise HUB / SWITCH / ROUTER gibi elemanlardan birine takılıdır.
➢ Bilgisayarınızı açınız ve MS-DOS komut istemine geçin.	➢ Bilgisayarınızın ağ kablosunun takılı durumda ve ağın kullanılabilir durumda olmasına dikkat ediniz.
➢ Komut satırında “IPCONFIG” yazarak bilgisayarınızın IP adres bilgilerini görün.	➢ Bu komut bilgisayarınızın IP ve ağ geçidi adres bilgilerini listeler.
➢ Görüntülenen listede  	➢ Varsayılan Ağ Geçidi yanında gösterilen IP adresi bilgisayarınızın internete çıkış için kullandığı cihaza ait IP adresidir.
➢ Bilgisayarınızda internet ya da ağ bağlantısını kullanan bütün programları kapatın.	Hiçbir bağlantı noktası kullanılmazken portlar dinleme modunda olacaktır.
➢ Şekildeki “NETSTAT -A” komutunu çalıştırın	➢ Bilgisayarınızda hiçbir bağlantı noktasının kullanılmadığını ve portların LISTEN konumunda olduğunu göreceksiniz

	
➢ Komut satırından CLS komutu ile ekranı silin ve “netstat 1.5” komutunu çalıştırın.	➢ Netstat komutundan sonra yazılan [1.5] parametresi her 1.5 saniyede bir bağlantı listesini sürekli yeniler. Durdurmak için CTRL+C tuş kombinasyonunu kullanabilirsiniz.
➢ İnternet Explorer penceresi açın ve bir dosya indirmeye başlayın.	Dosya indirirken siteye bağlantı yapılır ve dosya indirilmeye başlanır.
➢ Dosya inerken tekrar Komut satırına bakın. Bağlantıların kuruluşunu, karşılıklı anlaşmaları, dosya indirme sonunda karşılıklı bağlantı kapatma metotlarını kontrol edin.	➢ Dosya inerken bağlanılan siteyi, kullanılan protokolü ve sunucu ile karşılıklı kullandığınız portları göreceksiniz.
➢ Dosya indirme işlemi tamamlandıktan sonra bağlantı durumlarını önceki durumlarla karşılaştırın.	Bağlantılar sonlandırılırken FIN_WAIT1, FIN_WAIT2 ve TIME_WAIT durumlarını göreceksiniz.
➢ Aynı işlem basamaklarını Ağ üzerinde bulunan başka bir bilgisayar ile dosya paylaşımı yaparak tekrar ediniz.	Kullanılan protokole, bağlantı şekline ve portlara dikkat edin.

Öğretmeninizin ayrıca vereceği önerileri uygulama tablosuna not ediniz.

ÖLÇME VE DEĞERLENDİRME

Bu bölümde birinci öğrenme faaliyetinde verilen bilgilere hakimiyetinizi ve konuyu kavrama düzeyinizi ölçecek sorular sorulacaktır. Soruları bu düşünce doğrultusunda cevaplayınız.

OBJEKTİF TEST (ÖLÇME SORULARI)

Aşağıda verilen sorular için uygun cevap seçeneğini işaretleyiniz.

1. Aşağıdakilerden hangisi TCP/IP katmanlarından biri değildir?
A) Fiziksel Katman
B) İnternet Katmanı
C) Oturum Katmanı
D) Taşıma Katmanı

2. Aşağıdakilerden hangisi bir taşıma katmanı protokolüdür?
A) FTP
B) UDP
C) TELNET
D) SNMP

3. Aşağıdakilerden hangisi taşıma katmanının görevlerinden biri değildir?
A) Kaynak ve hedef portlar arası bağlantıları kontrol etmek.
B) Temel veri transferi.
C) Veri paketlerinin yönlendirilmesi.
D) Akış Kontrolü

4. TCP'de iletilen veri paketlerine ne ad verilir?
A) Datagram
B) Segment
C) URG
D) ACK

5. TCP ve UDP hakkında aşağıdakilerden hangisi yanlıştır?
A) İkisi de iletim protokolüdür
B) TCP yavaş, UDP hızlı iletim yapar.
C) TCP güvenli, UDP güvenli olmayan iletim sağlar.
D) UDP protokolünün veri paket yapısı daha karmaşıktır.

6. Bir UDP PDU aşağıdaki alanlardan hangisini içermez?
A) Sıra Numarası
B) UDP Başlığı
C) Ağ Arayüz Tanıtma Bölümü
D) Uygulama PDU

7. Aşağıdakilerden hangisi TCP veri paketinde bulunup UDP veri paketinde bulunmaz?
A) Veri Alanı
B) Kaynak Port
C) Pencere
D) Hata Kontrolü

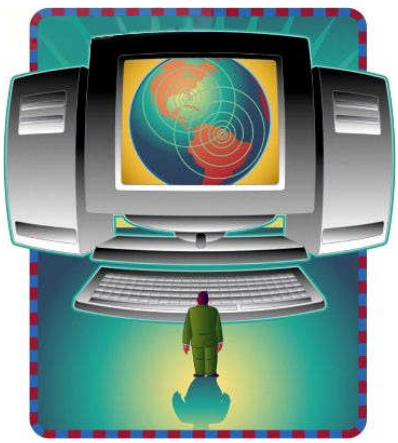
8. UDP protokolü TCP'ye göre neden hızlıdır?
A) Yapısı karmaşık olduğu için.
B) Öncelikli kullanıldığı için.
C) Alıcı taraf paketleri incelemediği için.
D) Gönderilen paketlerde onay alınmadığı için.

9. İletişim portu nedir?

A) Bilgisayarın bilgi kaydettiği bölümlerdir.
B) Bilgisayarların iletişim kurdukları bağlantı noktalarıdır.
C) Karşı bilgisayarın bilgileri kaydettiği bölümdür.
D) Bilgilerin iletildiği kablolardır.

10. TCP ve UDP protokollerinde kullanılan standart portlar kim tarafından belirlenir?

A) IANA
B) ASCII
C) DHCP
D) DNS



DEĞERLENDİRME -1

Sorulara verdiğiniz cevap seçeneklerini modül sonunda verilmiş olan cevap anahtarı ile karşılaştırınız. Kendinizi değerlendirdiğinizi unutmayınız. Yanlış cevapladığınız ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konular için bilgi sayfalarına tekrar dönerek eksiklerinizi gideriniz. Konu ilginizi çektiyse araştırma yaparak daha detaylı bilgi edinip kendinizi geliştirebilirsiz.

ÖĞRENME FAALİYETİ–2

AMAÇ

Uygulama katmanını işlevini kavrayarak, uygulama katmanının protokollerini kullanabileceksiniz.

ARAŞTIRMA

- Ülkemizde bir İnternet adresi alabilmek için başvurulan yerleri tesbit ediniz.
- Kullandığınız internet servis sağlayıcı hakkında bilgi toplayınız. Bu bilgileri sınıf ortamında arkadaşlarınızla paylaşınız.

2. TCP/IP UYGULAMA KATMANI

Bu bölümde, dört katmanlı TCP/IP mimarisinin en üst katmanını oluşturan uygulama katmanının kullanıcıya yakınlığını, bu katmanda iletim nasıl başlıyor, bu katman nasıl kullanılıyor, bu katmanda hangi protokoller hizmet veriyor, bu protokoller nasıl çalışıyor, bunların hepsini öğreneceksiniz. Beklide her zaman kullandığınız ama bu programların hiç bilmediğiniz veya düşünmediğiniz iletim şekillerini göreceksiniz. Sonuç olarak uygulama katmanı protokollerini daha etkin bir şekilde kullanabileceksiniz.

2.1. TCP/IP Uygulama Katmanı

Uygulama katmanı TCP/IP'nin kullanıcıya en yakın katmanıdır. Kullanıcının müdahale edebildiği, kullanabildiği yaya istediği bilgileri iletebildiği, diğer bilgisayarlara bağlantı kurabildiği uygulama programlarının bulunduğu katmandır. Örneğin dosya gönderip almak, web sayfalarında sörf yapmak, elektronik posta göndermek, İnternet üzerinde gerçek zamanlı sohbet etmek için kullandığı programların bu iletişimleri yapabilmesi için gerekli protokollerin hepsi bu katmanda bulunur.

2.2. UYGULAMA KATMANI PROTOKOLLERİ

Dördüncü ve en üst katman olan uygulama katmanında bulunan protokoller alt katmanda bilgi iletmek ya da almak için bir altta üçüncü katman olan taşıma katmanı protokolleri TCP ve UDP'yi kullanırlar. Göndermek istedikleri bilgileri uygun protokolü seçerek (TCP / UDP) bu bilgileri 4. ve 3. katman arasındaki önbelleğe koyarlar. TCP/UDP önbellekteki bu bilgileri alıp kendi kurallarına göre paketleyip bir attaki 2. katmana iletirler. 2. katmanda bulunan IP de paketlerin İnternet adreslerini üzerlerine ekleyip paketlerin yönlendirmesini yapar ve en alt fiziksel katmana gönderir. 1. katman olan fiziksel katman da verileri belirtilen adreslere fiziksel bağlantılar üzerinden iletir.

Karşı tarafın fiziksel katmanına ulaşan bilgiler ise bu defa yukarı katmanlara doğru gönderilir. 2. katman paketten İnternet adreslerini çıkartır 3. katmana gönderir. Burada TCP/UDP başlıkları çıkartılıp sadece veri kalır ve 3. ve 4. katmanlar arasındaki önbelleğe konulur. 4. katman olan uygulama katmanındaki ilgili program da önbellekten veriyi alarak kullanıcının kullanımına sunar.

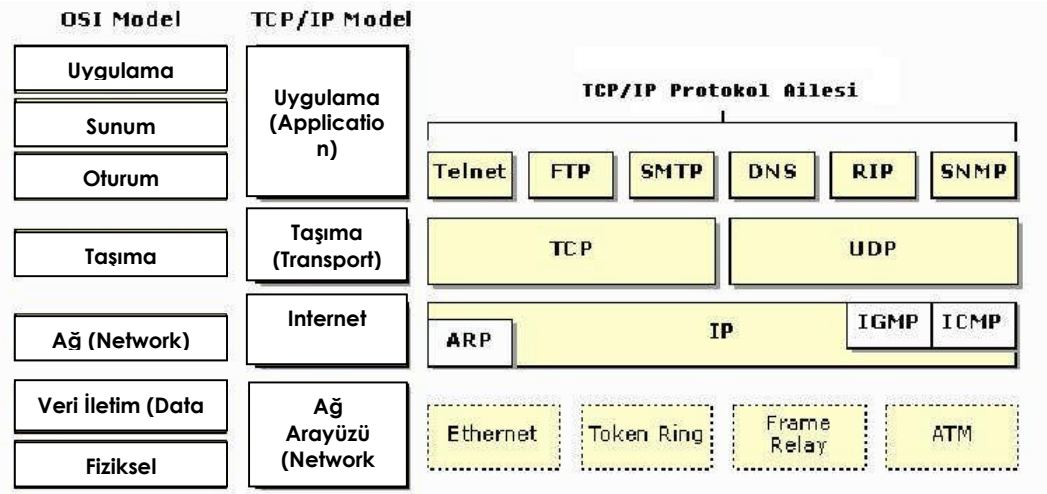
İletim bir uygulama programında başlayıp alt katmanlara gider. En alt katmanlar arasındaki fiziksel bağlantı ile karşı alıcıya iletilir. Karşıya ulaşan bilgiler sırasıyla üst katmanlara iletilerek en üst katmandaki uygulama katmanına ulaşır ve iletim tamamlanmış olur. Diğer bütün protokoller bu ara katmanlarda çalışır.

Şimdi uygulama katmanında çalışan protokollere bir göz atalım.

Hepimiz aslında interneti kullanırken bu protokolleri kullanmış oluruz ama birçoğumuz kullandığımızın farkında bile olmamışızdır.

Hepimiz İnternet üzerinden dosya indirir veya göndeririz. Bu işlemlere hepimizin bildiği gibi dosya indirme işlemine Download, gönderme işlemine ise Upload diyoruz. Download ve upload programlarının kullandığı protokol FTP'dir. Web sayfalarında İnternet Explorer, Opera, Mozilla, Netscape Navigator vb. programları kullanarak geziyoruz. Bu programlara Web Tarayıcı diyoruz. Web Tarayıcılar da web sayfalarını görüntülemek için HTTP protokolü kullanır. Günümüzde İnternet kullanıcılarının yaygın olarak kullandıkları e-postaların iletimi ve alımında kullandığımız programlar ve e-posta sunucuları ise SMTP protokolü kullanırlar. Yine orta ve ileri düzey bilgisayar kullanıcıları arasında yaygın bir uygulama olan TELNET de kendi adını taşıyan TELNET protokolü kullanır.

Saydığımız bütün bu uygulamalarda kullanılan protokollerin tamamı uygulama katmanında bulunurlar. Ayrıca bu katmanda çalışan bir de DNS (Domain Name System) vardır. İnternetin bel kemiği denilebilecek bu sistemin görevi; İnternet adreslerinin ve bu adreslerin bağlı bulunduğu IP adreslerinin kayıtlarını tutmaktır. Bağlanmak istediğiniz İnternet adresini çözümler ve sizi o adresin bağlı bulunduğu IP adresine yönlendirir. Böylece internette aradığınız siteye rahatlıkla ulaşabilirsiniz.



Şekil 13: TCP Protokolleri

2.2.1. DNS

İnternet erişiminde web adreslerini kullanırız. Bunlar bizim bildiğimiz www.meb.gov.tr, www.hotmail.com gibi internet adresleridir. Kullandığımız cep telefonlarında kayıtlı kişileri aramak için rehberden ilgili kişinin ismini seçip arama tuşuna basarız. Aslında aradığımız kişi değil numaradır. Telefonumuz rehber dosyasından isme karşılık gelen numarayı bulur ve bu numarayı arar. İnternet ortamında da durum bundan farklı değildir. Bağlantı kurup bakmak istediğimiz web sayfasının adresini yazar ve bağlanırız. Fakat iletişim isimle değil IP numaraları ile yapılır. Erişimde temel olan IP adresleridir. Peki IP adresleri ile erişim yapılıyorsa, neden biz harflerden oluşan internet adreslerini kullanıyoruz? Biz bu adreslere domain diyoruz ve domainler IP adreslerinin yerini tutarlar.

Telefon rehberimizde kayıtlı yüzlerce kişinin tamamının numaralarını aklımızda tutabilir miyiz? IP adresleri 0-255 arası değere sahip dörtlü sayı gruplarından oluşur (19.228.1.151). Tıpkı telefon numaraları gibi IP adresleri de dünya üzerinde tektir ve iki bilgisayar aynı IP adresine sahip olamaz. IP adresleri akılda kalıcı rakamlar değildir. Bu nedenle rakamlar yerine akılda kalması kolay olan web adresleri kullanılır.

İnsanlar isimleri tercih eder
meb.gov.tr

Bilgisayarlar ise rakamları
194.12.107.6

DNS (Domain Name System – Domain İsim Sistemi), domainleri IP adreslerine çevirmek için kullanılan bir sistemdir.

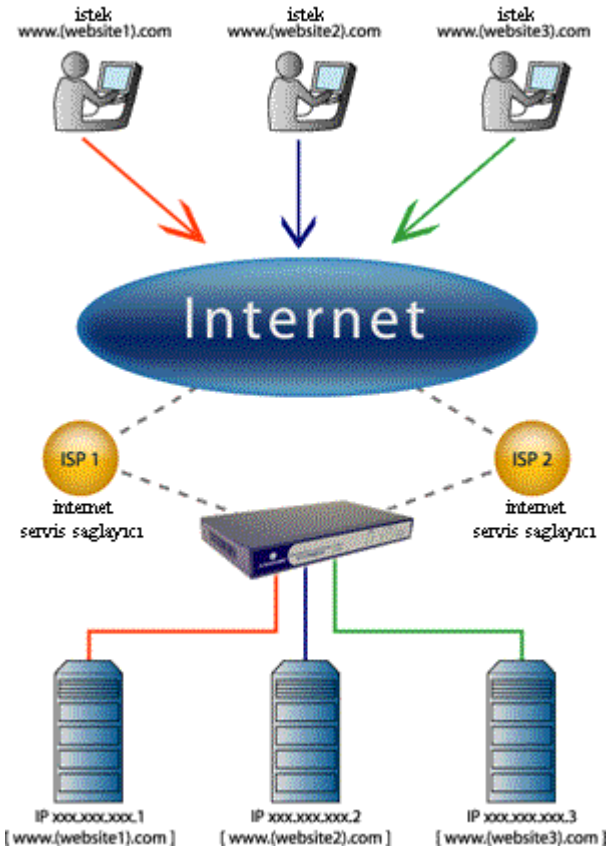
Web tarayıcılarda ve diğer uygulamalarda yazdığımız internet adresleri DNS kullanılarak IP adreslerine dönüştürülürler. DNS sunucular sorumlu oldukları bölgedeki bütün IP adreslerinin karşılık geldiği domainlerin kayıtlarını tutarlar. Bu isimler tam olarak tanımlanmış isimler de olabilir. örneğin "personel.meb.gov.tr" bu isimde "meb.gov.tr" domainin, "personel" ise bu domaindeki bir bilgisayarı ifade eder.

DNS sistemi 1984 yılında kuruldu. O döneme kadar IP adresleri host isimlerine HOSTS adında bit metin dosyası kullanılarak dönüştürülüyordu. Bütün host isimleri ve bunlara karşılık gelen IP adresleri bu dosyalara elle giriliyordu. İnternetteki bütün bilgisayarlarda bu dosyanın bir kopyası bulunuyordu.

Bir bilgisayar başka bir bilgisayarla iletişime geçebilmek için bu dosyaya bakıyor ve karşı bilgisayarın IP adresini bulup iletişim kuruyordu. Eğer o bilgisayarın kaydı dosyada yoksa iletişim kuramıyordu. Bu dosyanın sürekli güncel kalması gerekiyordu. Bu nedenle bu dosyanın yenilendiği ve kayıtlı bulunduğu ABD Stanford Univerty'den dosyanın güncel kopyasının alınması gerekiyordu.

İnternet yaygınlaştıkça bu durum içinden çıkılamaz bir hal aldı, dosya boyutu inanılmaz büyüdü ve yeni çözüm arayışına girildi. Bunun sonucunda 1984 yılında DNS sistemi kuruldu. Bundan önce tek bir noktada bulunan kayıtlar DNS sistemi ile artık İnternet üzerinde belirli bölgelere yetki dağıtımı ile birçok yere dağıtıldı.

DNS dağıtılmış bir yapıya kavuşması için bilgisayarlar gruplandırılmaya başlandı. Örneğin ".tr" domaini Türkiye'deki DNS sunucu, uzantısı olmayan ".com" domaini ABD'deki ticari kuruluşların kayıtlarını tutan DNS sunucu, ".de" domainlerini Almanya'daki DNS sunucunun tutması gibi.

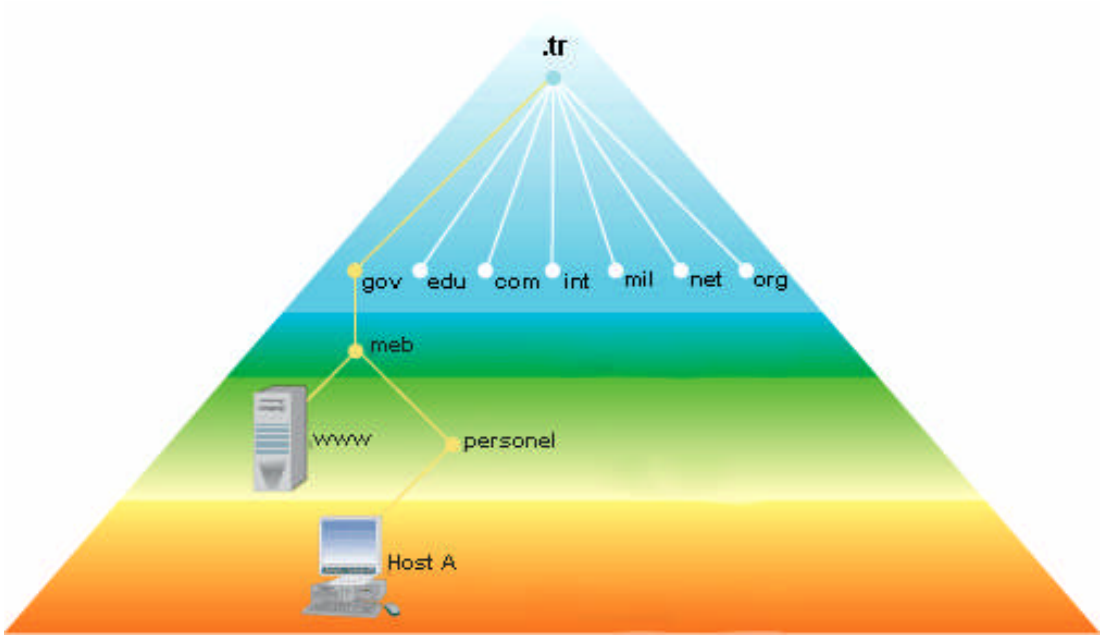


Şekil 14: DNS Erişim Yapısı

Bu DNS sunucularında aynı domain iki farklı kişiye verilmez. Domain isimleri de IP adresleri gibi tektir. Web tarayıcınızda bir internet adresi girdiniz ve bağlanmaya isteğinde bulundunuz. Bu öncelikle bağlı bulunduğunuz bölgedeki DNS sunucuya gider. Eğer bağlı bulunduğunuz DNS sunucu, domain kayıtlarında istediğiniz adrese karşılık gelen IP adresini bulur ve size gönderir. Eğer bulamazsa, sizi bulabilecek bir başka DNS sunucusuna gönderir. Bu DNS sunucu bulursa, size IP adresini gönderir, bu da bulamazsa başka bir DNS sunucusuna gönderir. Zaman aşımı süresi dolana kadar bu şekilde devam eder. Süre dolmuşsa ve domaine ait IP adresi bulunamamışsa kullanıcıya hata mesajı gönderilir ve kullanıcı bilgilendirilir. Eğer web sitesi bulunamamışsa tarayıcınız size “Unable to locate the server or there was a DNS error” “Sunucuya ulaşılamıyor veya DNS hatası var” mesajı verecektir.

2.2.1.1. DNS Hiyerarşisi

Bir DNS, DNS sunucular ve çözümleyicilerden oluşur. Sunucular Host ve IP adresi eşleştirmelerini tutar, çözümleyici ise sadece DNS sunucuların adreslerini tutar. Bir istemci bir adrese ait IP adresini bulmak istediğinde isim sunucuya (Name Server) başvurur. Sunucu adres kendi veritabanında varsa bunu istemciye gönderir.



Şekil 15: DNS Yapısı

İnternet adresleri sondan başa doğru çözümlenir ve öncelikle ülkelere ayrılırlar. .tr, .uk. de.nl gibi uzantılar, adreslerin bulundukları ülkeleri ifade eder. Örneğin tr Türkiye'yi, de Almanya'yı, nl Hollanda'yı, uk İngiltere'yi ifade eden eklerdir. Bütün ülkeler için bir takı bulunurken ABD için herhangi bir takı kullanılmaz. Bu nedenle eğer adreslerin sonunda ülke takısı yoksa bu adresin ABD'de bulunduğu varsayılır. Örneğin www.unicef.org, www.un.org gibi adreslerin Amerika'da bulunduğu varsayılır.

İnternet adresleri ülkelerden sonra com, edu, mil, gov gibi bölümlere ayrılır. Bu bölümlere üst düzey (top-level) domainler denir. Bu domainlerin ifade ettikleri bölümler şunlardır.

- .com : Ticari kuruluşlar (COMmercial)
- .edu : Yüksek öğrenim kurumlar (EDUcation)
- .org : sivil toplum kuruluşlar (ORGanizations)
- .gov : Hükümete ait kurumlar (GOVernment)
- .mil : Askeri kurumlar (MILitary)
- .net : Büyük ağ hizmetleri veren kuruluşlar (NETwork)
- .int : Uluslar arası organizasyonlar (INTernational)
- .num : Telefon numaraları bulabileceğiniz yerler (NUMbers)
- .arpa : Ters DNS sorgulaması yapılan yerler.

2.2.1.2. DNS Sunucular ve Çeşitleri

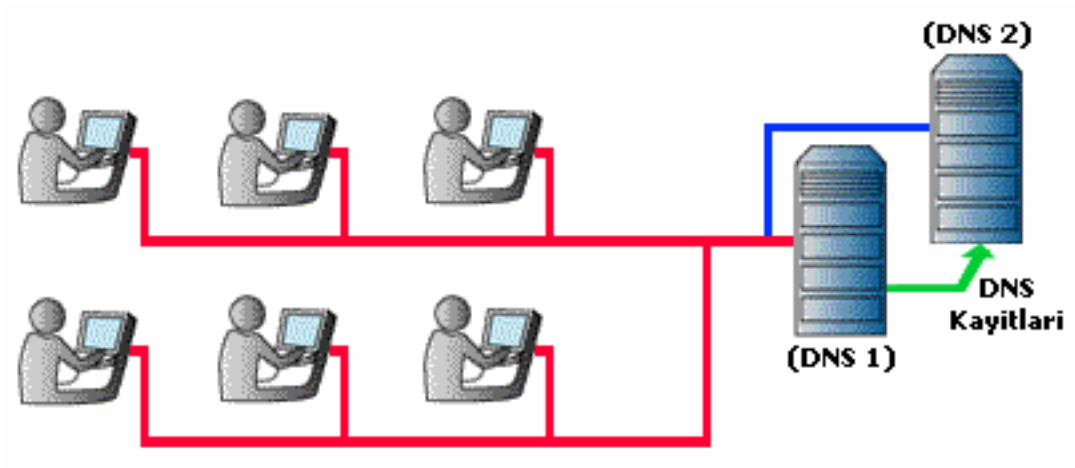
DNS sunucular kendi sorumluluk bölgelerindeki domainleri ve bu domainlerin bulunduğu bilgisayarların IP adreslerinin kayıtlarını tutarlar.

Çalışmalarına göre DNS sunucular üçe ayrılırlar.

- Birincil İsim Sunucu (Primary Name Server)
- İkincil İsim Sunucu (Secondary Name Server)
- Yalnızca Önbelleğe Alan İsim Sunucu (Cache-Only Name Server)

Birincil İsim Sunucu (Primary Name Server)

Sorumlu olduğu bölge ile ilgili bilgiler zone.host isimli bir dosyada tutar. Bu dosyaya bilgiler tek tek elle girilir. O bölgede bulunan bilgisayarlara DNS sunucu adresi olarak birincil DNS sunucu adresi girilir. Böylece IP çözümlemek için başvuran bilgisayar öncelikle kendisine en yakın olan bu DNS sunucuya gidecektir.



Şekil 16: İkincil DNS Çalışma Yapısı.

İkincil İsim Sunucu (Secondary Name Server)

Eğer sunucu sorumluluğundaki bölgede çok sayıda bilgisayar varsa IP çözümleme hızında düşme olacaktır. Bunu önlemek için yapacağımız ilk iş ikinci bir DNS sunucu kurup bu sunucuya da bilgileri tek tek elle girmek olacaktır. Fakat çok fazla bilgisayar olduğu için elle girme işini tekrar yapmak zahmetli olur. Ayrıca her iki sunucunun da kayıtlarını sürekli güncel tutmak gerekir. Çok zahmetli ve hata oluşturabilecek bir yöntem olacaktır. Bu nedenle ikincil bir DNS sunucu oluşturulmuştur.

İkincil DNS sunucuya sorumlu olduğu bölge ile ilgili bilgiler elle girilmez. Bilgileri bağlı olduğu bir başka DNS sunucudan alır. Bağlı bulunduğu DNS sunucu birincil DNS sunucu da olabilir başka bir ikincil sunucu da olabilir.

Yalnızca Önbelleğe Alan İsim Sunucu (Cache-Only Name Server)

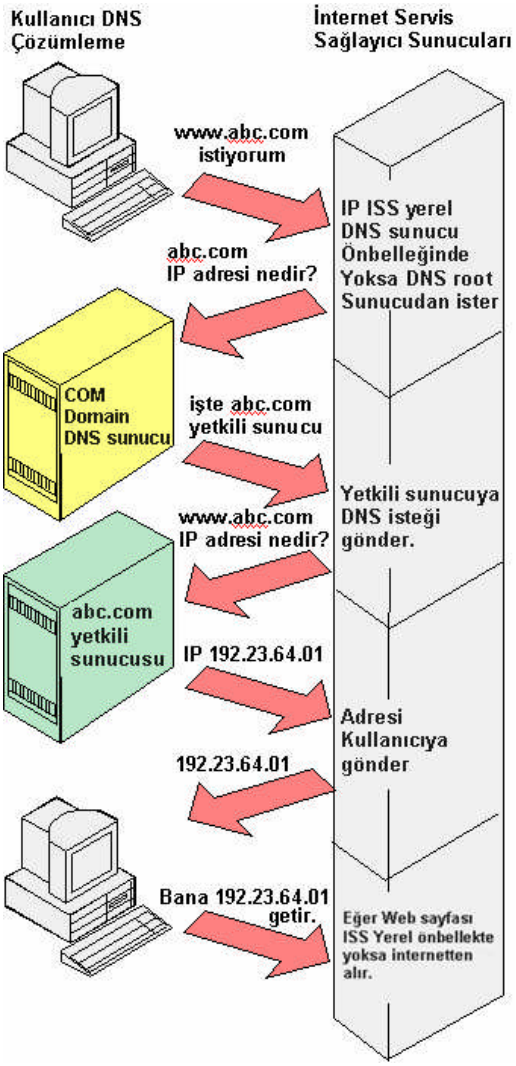
Bu sunucuda ait olduğu bölge kayıtlarının bulunduğu dosya kesinlikle bulunmaz. Bağlı bulunduğu bir üst DNS sunucu vardır. Kendisine yapılan istekleri bu sunuculara sorar ve aldığı bilgileri istemciye ulaştırır. Aynı istek tekrar yapılabilir diye bu bilgileri atmaz. Bir sonraki istekte daha hızlı yanıt vermek için bu bilgileri önbelleğinde tutar.

2.2.1.3. DNS Çözümleme

Kullanıcı bağlanmak istediği web adresini internet tarayıcıda yazarak açmak istediği zaman sayfalara ait dosyalar kullanıcı bilgisayarına indirilir. Kullanıcı bilgisayar ve web sunucu arasında bir bağlantı olmadan dosya transferi mümkün değildir. Ayrıca web adresleri kullanıcılar içindir. Bilgisayarlar web adresleri kullanmazlar. IP adresleri ile iletişim kurarlar. Bu nedenle girdiğimiz web adresine ait IP adresinin bulunması gerekmektedir.

Girdiğimiz web adresleri öncelikle bağlı bulunduğumuz İnternet Servis Sağlayıcı (ISS) DNS sunucusuna iletilir. ISS'ye bağlı diğer kullanıcılardan birisi daha önce bu adrese bağlanmışsa ISS DNS sunucu önbelleğinde bu adrese ait IP adresi vardır ve derhal IP adresi kullanıcıya gönderilir. Eğer IP adresi önbellekte bulunamazsa DNS kök sunucusuna web adresinin son ekine göre yetkili DNS sunucunun hangisi olduğunu öğrenmek için istekte bulunur. Aşağıdaki örnekte .com kök sunucusuna abc.com yetkili sunucusu için istekte bulunulmuştur.

DNS kök sunucu yetkili DNS sunucu bilgisini ISS'ye gönderir. ISS bu defa web adresi için yetkili sunucudan IP adresi ister. Yetkili sunucu IP adresini bildirir. ISS bu IP adresini kullanıcıya iletir. Kullanıcı artık IP adresini öğrenmiştir. Bu defa IP adresine ait web sayfası için istekte bulunur ve ISS bu web sayfasına ait bilgileri kullanıcıya iletir. Böylece bir web sitesi görüntülenmiş olur.



Şekil 17: DNS Çözümleme İşlemi

2.2.2. FTP VE TFTP

Bir bilgisayardan diğerine dosya göndermek ağ kullanımının en önemli işlevlerinden biridir. Bu işler için e-posta eklentilerinden faydalanabilirsiniz. Bu dolaylı yoldan yapılan bir işlemdir. Öncelikle dosya e-posta sunucusuna gider ve alıcının posta kutusuna kaydedilir. Doğrudan yapılan dosya transferi kadar etkin bir yol değildir. Eğer daha hızlı ve etkili bir sonuç istiyor ve alıcının dosyayı hemen almasını istiyorsanız, dosya iletim protokolleri kullanmalısınız. Bu protokoller FTP ve TFTP olmak üzere iki adettir. FTP (File Transfer Protocol – Dosya İletim Protokolü) ve TFTP (Trivial FTP – Önemsiz Dosya Transfer Protokolü) dosyaları bir bilgisayardan diğerine kopyalamak için kullanılır. Şimdi bu protokolleri ayrı ayrı inceleyelim.

2.2.2.1. FTP ile Dosya Transferi

FTP bir TCP/IP uygulamasıdır. Bu da FTP'nin 4. TCP katmanında bulunduğunu gösterir ve dosya iletimi için TCP kullanır. FTP Amerika Savunma Bakanlığının 1960'lardan 1980'lere kadar kullandığı ARPANET' üzerinde çalışan eski bir protokoldür. Öncelikli görevi; bilgisayarlar arasında kararlı ve güvenilir bir şekilde dosya transfer etmektir. FTP bu güvenilirliği ve kararlılığı İnternet üzerine taşıyarak günümüzde de halen sürdürmektedir.

Önceleri www şimdi olduğu gibi popüler değilken dosya transferleri için insanlar komut satırı uygulamaları kullanırlardı. O dönemlerde FTP kullanmak için komut satırından komutlar girilirdi. Şimdi ise web tarayıcıları FTP kullanarak dosya indirme işlemlerini yapabilmektedir.

FTP genellikle dosyaları uzak bilgisayarlarda depolamak için kullanılır. Bu sizin bir bilgisayar sisteminde çalışırken dosyalarınızı başka bir sistem üzerinde depolamanıza olanak tanır. Örneğin bir web sayfası hazırladınız. Bu web sayfasını yayınlamak için dosyalarınızın uzak bir web sunucuda satın aldığınız alana gönderilmesi ve orada saklanması gerekir. İşte bu dosyaları gönderme işlemi için bir FTP uygulaması ile FTP protokolü kullanırsınız.

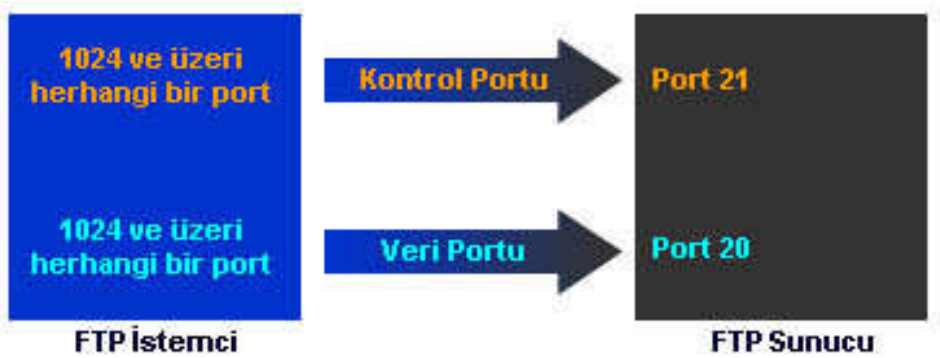
Sizin bilgisayarınızda, web sunucu bilgisayarın kullandığından farklı bir işletim sistemi bulunabilir. Bu durumda dosyalarınızı nasıl göndereceksiniz? Aynı işletim sistemi kullanan bir web sunucusu mu bulmak zorundasınız? FTP ile böyle bir sınırlandırma ortadan kalkıyor. Çünkü FTP'nin en önemli özelliği, farklı donanım ve işletim sistemleri üzerinde çalışabilmesi ve dosya kopyalama işlemi yapabilmesidir.

Ayrıca web sunucuda satın aldığınız alana başka kişilerin dosya göndermesi yada sizin sayfanızı oluşturan dosyaları silmesini istemezsiniz. Sizden başkası bu alana girmemelidir. Bu nedenle web sunucunun, sizin bu alana erişiminize izni vermesi için sizi tanıması gerekir. Sizi tanıyabilmesi için de bu alanı satın alırken size bir kullanıcı adı ve şifre verilir. Sizin güvenliğiniz için kullanıcı adı ve şifre girilmeden bu alana kimse erişemez. Kimse bu alandan FTP ile dosyalarınızı alamaz, silemez ve değiştiremez. FTP ile bu alandan dosya almak ve bu alana dosya göndermek için bir dizi işlemi yerine getirmek gerekir.

- Bir FTP servisini kullanabilmek için bir FTP istemci uygulaması açılır.
- Bağlanılacak olan FTP sunucunun IP adresi ilgili alana girilir.
- Bu sunucuya bağlanmak için yetkili kullanıcı adı ve şifre sorulur.
- Kullanıcı adı ve şifre ilgili pencerede girilerek FTP sunucuya bağlanılır.

2.2.2.1.1 FTP Bağlantıları

Bir FTP bağlantısı açtığınızda port 20 ve port 21 olmak üzere iki porta birden bağlanırsınız. Bu iki port iki farklı işleve sahiptir. Port 20, veri portudur, port 21 ise kontrol portudur.



Şekil 18: FTP İstemci ve Sunucu Bağlantısı.

Kontrol Portu

Kontrol portu, FTP'de komut ve bu kotlara verilen yanıtların iletimi için kullanılır. İstemci komut gönderir ve sunucu bu komutlara 21 numaralı port üzerinden yanıt verir.

Eğer FTP ile GET DOYSA gibi bir komut göndermişseniz alacağınız sunucu yanıtı şöyle olacaktır:

200 PORT command successful.
150 Opening ASCII mode data connection for .message (127 Bytes)
226 Transfer comlete.
local: .message remote: .message
135 bytes received in 1.4 seconds (0.09 KB/s)

Dikkat ederseniz sunucu kullandığı komutların önüne PORT komutu ekleyerek gönderiyor. Bu da veri portu yerine 21 numaralı kontrol portunun kullanılacağını gösterir. Bazı FTP uygulamalarında veri portundan da komut gönderilir fakat bu komutlar pasif (PASV) komutlardır. Kontrol komutları (PORT) 21 numaralı porttan gider.

PASV komutunun gerçekte kullanım amacı, FTP'yi firewall dostu yapmaktır. Dosya aktarımı için istemci taraf kendisine bir port seçer. Seçtiği portu FTP sunucuya bağlantı isteğinde bulunması için PORT komutu ile bildirir. FTP sunucu bu istemci portuna bir bağlantı isteği gönderir ve bağlantı kurulur. Bu bağlantıya genellikle Geri Bağlantı (Back Connection) adı verilir.

Sunucunun bağlantı noktası sürekli sabittir. Fakat istemcinin bağlantı noktası 1024 – 65535 arası portlardan rastgele seçilmiş geçici bir noktadır. Firewall dışardan saldırılara karşı 0 – 1023 portları hariç, 1024-65535 arası portların tamamını dışardan gelen isteklere kapatır. FTP sunucu bu nokta ile bir bağlantı yaratmak için istekte bulunacaktır. Fakat firewall istekte bulunulan port 1024-65535 arasında olduğu için isteğe izin vermez ve FTP sunucu bağlantıyı yaratamaz.

Bu problem FTP sunucuyu pasif konuma geçiren PASV komutu ile çözülür. Sunucu pasif olunca bağlantı kurma işi istemciye kalır. Çünkü firewall, portları yalnızca gelen bağlantı isteklerine kapatır. Giden bağlantı isteklerine her zaman izin verir. İstemci 1024-65535 arası bir port seçip sunucuya bağlantı isteğinde bulunur. Sunucu bu portu görür ve PASV ile kendi portunu söyler pasif konuma geçer. İstemci PASV komutunu görünce sunucunun pasif olduğunu anlar ve sunucu portuna aktif FTP bağlantısı isteğinde bulunur. Sunucu kabul eder ve istemci aktif bağlantıyı kurmuş olur.

Veri Portu

Veri portu FTP verilerinin (dosya) gönderildiği 20 numaralı porttur. Bu port 21 numaralı, kullanıcının sunucuya komut gönderdiği kontrol portundan farklıdır. Dosyalar FTP ile aktarılırken bu porttan komutlar değil, dosyaların kendisi geçer.

Veri portuna yapılan bağlantılar kendine ait komut setine sahip pasif bağlantılardır. Bağlantıya hazır bir şekilde beklenirken, pasif veri işlemi kontrol işleminden bir yapılacak herhangi bir veri bağlantı çağrısı için 20 numaralı veri portunu dinler. Kontrol bağlantısı ile birlikte aynı anda pasif veri bağlantısı da açılır. Bu durumda, komutlar kontrol portuna gelir. Fakat, veri portunu da pasif FTP komutlarıyla kontrol edebilirsiniz.

Pasif FTP Komutları

PASV komutu kullanıcının kullandığı bir komut değildir. Kullanıcı tarafın çalıştırabildiği komut PORT komutudur. Fakat FTP bağlantı yapıldıktan sonra pasif komutların da bir kısmının kullanılmasına izin verir.

Bu komutları kullanabilmek için port 21'e şu şekilde bir TELNET bağlantısı yapabilirsiniz:

```
o ftp.batl.k12.tr 21
Bağlanıyor ftp.batl.k12.tr
220 batl.k12.tr FTP
user kullanici_adi
331 Password required for kullanici_adi
pass sifre
```

TELNET kullanarak yukarıdaki şekilde 21 numaralı porta bağlantı kuruluyor. Bağlantı kurulduktan sonra bağlanılan FTP sunucusu bağlantı kurulduğuna dair 220 numaralı kodla bir mesaj gönderir. Bu mesajdan sonra user komutu ile kullanıcı adınızı ve pass komutu ile şifrenizi girmelisiniz. Burada şifre girerken dikkat edin. Çünkü yazdığınız şifre ekranda görünmediği gibi * işareti ile de gösterilmeyecektir.

```
230 User kullanici_adi logged in
```

Kullanıcı adı ve şifre onaylandıktan sonra yukarıdaki mesajı alırsınız ve hemen ardından ftp> promptu ekranınıza gelir. Artık FTP sunucusuna bağlısınız. Artık FTP komutlarını girerek dosya transferi yapabilirsiniz.

2.2.2.1.2. Standart FTP Komutları

Komut	Görevi
CD	Dizin değiştirir (cd <dizinadi>)
PWD	Bulunulan dizini gösterir.
DIR	Bulunulan dizindeki dosyaları listeleme
LS	Bulunulan dizindeki dosyaları kısa bir şekilde listeleme
GET	Dosya alma (get <dosya adı> <alındıktan sonra verilecek ad"kullanılmayabilir">)
PUT	Dosya gönderme (put <dosya adı> <sunucudaki dosya adı>)
MGET	Çoklu dosya alma (mget a*.*) "a ile başlayan dosyaları al"
MPUT	Çoklu dosya gönderme (mput *.exe) "bütün exe uzantılı dosyaları gönder"
ASCII	ASCII aktarım moduna geçer.
BINARY	BINARY aktarım moduna geçer.
DELETE	Sunucuda (yetkiniz varsa) dosya siler (delete <dosya adı>)
MKDIR	Sunucuda (yetkiniz varsa)dizin oluşturur (mkdir <dizin adı>)
RMDIR	Sunucudaki bir dizini siler (rmdir <dizin adı>)
LCD	FTP ortamından çıkmadan kendi bilgisayarınızda dizin değiştirmenizi sağlar.
CLOSE	FTP ortamından çıkmadan bağlantıyı keser.
QUIT	Bağlantıyı keser ve FTP ortmından çıkar.
HELP	Kullanılabilecek komutlar hakkında yardım gösterir.

Tablo 7: Standart FTP komutları.

Komutları aişağıdaki örneklerde olduğu gibi kullanabilirsiniz.

```
ftp> pwd                ftp> get notlar
/home/dokumanlar        200 PORT command successful.
ftp>                    150 ASCII data connection for notlar (1.2.3.4,52264)(210 bytes).
                        226 ASCII Transfer comlete.
                        Local: notlar remote: notlar
                        226 bytes received in 0.019 seconds (11.81 Kbytes/s)
                        ftp>
```

2.2.2.2. TFTP (Trivial FTP)

TFTP, LAN üzerinde kullanıma daha uygundur. FTP'nin küçültülmüş hali olarak da düşünülebilir. FTP, TCP iletimi kullanırken TFTP daha basit ve hızlı olan UDP iletimi kullanılır. UDP kullanımı da TFTP'yi biraz güvensiz hale getirebilir.

TFTP, dosya aktarımı için kullanılan bir uygulama katmanı protokolüdür. UDP veri portu olan 69 numaralı portu kullanır. TFTP, FTP gibi kullanıcı adı ve şifresi gibi yetkili giriş gerektirmez. Bu yüzden güvenlik sorunları vardır.

Günümüzde genellikle terminalden routere, router erişim listelerinin gönderilmesi için veya router ayarlamaları için kullanılır. Bazen ağ üzerinde kendine ait bir sabit diski olmayan bilgisayarlar da olabilir. bu bilgisayarların açılabilmeleri için gerekli işletim sistemi dosyalarını ağ üzerindeki bir bilgisayardan alması gerekir. Bu dosyaları indirip belleğine yüklediği kaynak TFTP sunucudur. Bu dosyaları da TFTP kullanarak hızlı bir şekilde kendisine aktarır. TFTP'nin FTP'ye karşı avantajı; daha basit bir yapıya sahiptir.

TFTP iletiminde istemci ve sunucu arasındaki her paket değişimi istemcinin sunucudan okuma veya yazma isteğinde bulunmasıyla başlar. Dosya transferleri oktet (bayt) veya netASCII modunda yapılır. NetASCII modunda veri satırları 255 karakterlik ASCII karakter setinden oluşur ve <enter> işaretiyle ayrılır.

TFTP ve FTP Arasındaki Farklar

TFTP, FTP kadar işlevsel değildir. Örneğin, TFTP'de dizin oluşturma/silme, dosya silme gibi işlemler yapma imkanınız yoktur. Bağlantı kurduğunuzda sizden kullanıcı adı veya şifre istemez. Güvenlik açığı çoktur. Basit yapısı nedeniyle routerler erişim listelerini ve konfigürasyon bilgilerini bu protokolü kullanarak iletir.

TFTP Komutları

Eğer FTP'yi anlamışsanız, TFTP sizin için zor olmayacaktır. TFTP çok az bir komuta sahiptir. Bu komutlar aşağıdaki tabloda listelenmiştir.

Komut	Görevi
ascii	netASCII (metin) aktarım moduna geçer.
binary	BINARY aktarım moduna geçer.
connect	TFTP sunucya bağlanır.
mode	Dosya transfer moduna geçer.
get	Uzak sunucudan dosya alır.
put	Uzak sunucuya dosya gönderir.
quit	TFTP'den çıkar.
Rexmt <değer>	Her paket için ayrı zaman aşım süresi belirler.
status	Sunucu durumunu gösterir.
timeout <saniye>	İletim zaman aşımını saniye cinsinden belirler.
trace	Paket takibini etkinleştirir.
verbose	Gereksiz paketleri etkinleştirir.

Tablo 8: TFTP Komutları.

Sonuç olarak dosya transferi, bir TCP/IP ağında farklı sistemlere sahip terminallere dosya göndermek için önemlidir. TCP/IP ağ üzerinde dosya göndermek için öncelikli olarak Dosya İletim Protokolü (FTP) ve TFTP kullanır.

TCP kullanan FTP, dosya iletimi için iki port kullanır (Veri Portu 20 ve Kontrol Portu 21) ve bunların açık olması gerekir. Veri portu yalnızca dosyaların iletimi için kullanılır. Kontrol portu ise komut mesajları için kullanılır.

UDP kullanan TFTP ise 69 numaralı portun açık olmasını gerektirir. TFTP, FTP'den daha basit yapılı bir protokoldür. Fakat çok fazla fonksiyonel değildir. Bununla beraber, TFTP routerlerin erişim listelerini yönetmek ve ayarlamalar yapmak için. Aynı zamanda da sabit diski bulunmayan sistemlerin boot işlemlerini yapabilmeleri için kullanır.

2.2.3. HTTP (HyperText Transfer Protocol)

HTTP, Web sunucular ve Web Tarayıcı (Internet Explorer, Mozilla, Opera vb.) arasında Web üzerinden veri Transferi yapmalarını sağlayan bir protokoldür. İstek/yanıt ilkesi ile çalışır. Sunucu bekler, kullanıcılardan gelen isteklere yanıt verir. HTTP, kullanıcı ile bir bağlantı oluşturmaz. HTTP daha çok, 80 numaralı TCP portu üzerinden güvenilir TCP bağlantılarını kullanır. Bu kullanıcı/sunucu işlemleri dört temel adımda gerçekleşir:

- Web Tarayıcı sunucuya bağlanır.
- Tarayıcı sunucudan belgeler için istekte bulunur.
- Sunucu tarayıcıya yanıt verir.
- Bağlantı sona erer.

HTTP pasif bir protokoldür. Bu nedenle kendisi bağlantı kurmaz ve bağlantı durumuyla ilgilenmez. Sadece kendisine gelen istek doğrultusunda, istenilen belgeleri gönderir.

Bu başlıkta HTTP'nin v1.1 standart versiyonundan, HTTP ile sunucu – tarayıcı iletişiminden, web sunucularındaki web sayfalarına nasıl ulaşıldığından, ve URL kavramından bahsedilecektir.

2.2.3.1. URL Kavramı

İnternet üzerindeki sunucu bilgisayarlarda milyonlarca web sayfası, milyonlarca dosya var. Bu sayfalara, bu dosyalara nasıl ulaşıyoruz? Nerde olduğunu bilmediğimiz bir sunucudaki web sayfasına nasıl ulaşıyoruz?

Web, web sayfalarını ve diğer kaynakları tanımlamak için URL (Uniform Resource Locators) adında bir şema kullanır. Bir URL şemasında neler bulunur, bir örnekle birlikte inceleyelim.

http://www.meb.gov.tr/meb/teskilat.html

Bu URL'de sizi World Wide Web birliğindeki bir web sayfasına götüren kısımlar şunlardır:

- Kullanılan protokol HTTP'dir
- Tam domain adı "www.meb.gov.tr"
- Dizin "meb"
- Alınacak dosya "teskilat.html"

Çoğu zaman yalnızca tam domain ismini kullanırız. Web sunucular domain ismi ile çağırılan web sayfalarında otomatik olarak "index.html, default.html, home.htm, index.htm" sayfalarından hangisi varsayılan olarak belirlenmişse o dosyayı getirecektir. Bu nedenle çoğu zaman dosya adı yazmadan yalnızca http://www.meb.gov.tr yazmamız yeterli olmaktadır.

Diğer yaygın URL örnekleri ise şunlardır.

ftp://sunucu_adi/dizin/dosya_adi
ftp://kullanici_adi@sunucu_adi/dizin/dosya_adi
telnet://sunucu_adi
news://habersunucu_adi/haber_grubu

Bu örnekler sırasıyla, anonim bir FTP'den bir belge, kullanıcı adı kullanarak bir FTP'den bir doküman, bir TELNET erişimi, Usenet haber grubuna erişim isteklerini göstermektedir.

2.2.3.2. HTTP / 1.1

HTTP protokolü, sunucu ve kullanıcı arasında bir bağlantının kurulabilmesi için istek ve cevap mesajlarına uygun hazırlanmış bir web dili belirler.

Kullanıcı isteği ve sunucunun bu isteğe verdiği cevap belirli bazı özellikleri taşımak zorundadır. Bu özellikler aşağıda açıklanmıştır.

Kullanıcı İsteği

Kullanıcı istek mesajında bulunması gereken bazı bilgiler vardır. Bu bilgiler sunucuya ulaşmazsa, sunucu isteğe yanıt vermeyecektir. Bu bilgiler:

- İstek Metodu
- İstek Başlığı
- İstekte Bulunulan Bilgi

İstek metodu

Belirtilen URL yada web sayfasına uygulanacak olan programdır. Aşağıdaki tabloda kullanılabilir istek metotları listelenmiştir.

Metot	Açıklama
GET	Belirli bir belgeyi ister.
HEAD	Sadece sayfa başlığını ister.
POST	Sunucunun belirtilen belgeyi çalıştırılabilir kabul edip bazı bilgileri göndermesi için yapılan istektir.
PUT	Kullanıcıdan gelen verilerle belirtilen dosya verilerini değiştirir.
DELETE	Sunucunun belirtilen sayfayı silmesini ister.
OPTIONS	Kullanıcının sunucun gereksinimlerini ve yeteneklerini görmesine olanak tanır.
TRACE	Test amaçlı kullanılır. Kullanıcının mesajları nasıl aldığını görmesine izin verir.

Tablo 9: HTTP İstek Metotları.

Başlık Bilgisi

Seçimliktir. Sunucuya kullanıcı hakkında ek bilgiler sağlayan bir bölümdür. Kullanma zorunluluğu yoktur. Bu bilgileri sağlayan istek başlıkları aşağıdaki tabloda belirtilmiştir.

Başlık	Açıklama
Accept	Kullanıcının kabul edeceği veri tipi.
Authorization	Kullanıcı adı ve şifresi gibi yetkisel bilgiler içerir.
User-Agent	Kullanıcının kullandığı Web Tarayıcı yazılımı.
Referer	Kullanıcıyı buraya gönderen web sayfası.

Tablo 10: İstek Başlıkları.

İstekte Bulunulan Bilgi

Eğer uygulanan metot kullanıcıdan bilgiler gerektiriyorsa (örneğin, POST) kullanıcı başlığın hemen arkasından gerekli bilgileri gönderir. Aksi halde kullanıcı sunucudan yanıt beklemeye devam eder.

Sunucu Cevabı

Sunucunun verdiği cevaplar da birçok anahtar nesneler içerir. Bu nesneler:

- Durum Kodu
- Cevap Başlığı
- Cevap olarak gönderilen veri

Durum Kodu: HTTP tarayıcı ile iletişime tekrar devam edebilmek için birçok durum kod grubu tanımlar. Bu kodlar aşağıdaki tabloda listelenmiştir.

KOD	Açıklama
Bilgilendirme Amaçlı (1xx)	
100	Devam et
101	Protokol değiştiriliyor
Başarılı Bildirimler (2xx)	
200	Tamam (Başarılı)
201	Yaratıldı
202	Kabul Edildi
203	Güvenli olmayan bilgi
204	İçerik yok
205	İçeriği yeniden gönder
206	İçeriğin bir bölümü
Yeniden Yönlendirmeler (3xx)	
300	Çoklu Seçim
301	Kalıcı olarak taşındı
302	Geçici olarak taşındı
303	Diğerlerine bakınız
304	Düzenlenmedi
305	Proxy kullan
Sunucu Hataları (5xx)	
500	Dahili sunucu hatası
501	Tamamlanamadı
502	Geçersiz Gateway (Geçit)

KOD	Açıklama
Kullanıcı Hataları (4xx)	
400	Hatalı istek
401	Yetkiniz yok
402	Ödeme gerekmektedir (Ücretli)
403	Yasak
404	Bulunamadı
405	Bu metodun kullanımına izin yok
406	Kabul edilemez
407	Proxy doğrulaması gerekiyor
408	İstek zaman aşımına uğradı
409	Uyuşmazlık
410	Gitti
411	Uzunluk gerekli
412	Önkoşul başarısız
413	İstekte bulunulan varlık çok büyük
414	İstekte bulunulan URL çok uzun
415	Desteklenmeyen ortam biçimi
503	Servis kullanılamaz
504	Gateway (Geçit) zaman aşımı
505	HTTP sürümü desteklenmiyor

Tablo 11: HTTP Durum Kodları.

Cevap Başlığı: Kullanıcıya sunucu hakkında ve/veya istekte bulunduğu belge hakkında bilgi sağlar. Kullanılan cevap başlıkları aşağıda listelenmiştir:

Metot	Açıklama
Server	Web sunucu hakkında bilgi
Date	Şu andaki aktif tarih/saat
Last-modified	İstenilen belgenin son güncellendiği tarih/saat
Expires	İstenilen belgenin geçerlilik süresi (tarih/saat)
Content-type	Verinin MIME tipi.
Content-length	İçerik boyutu (bayt olarak)
www-authenticate	Yetki için gerekli bilgileri (kullanıcı adı, şifre vb.) kullanıcıya iletmek için kullanılır.

Tablo 12: Sunucu Cevap Başlıkları.

Eğer kullanıcı veri isteğinde bulunmuşsa, veri bu kısmı takip edecektir. Aksi halde sunucu bağlantıyı kapatacaktır.

MIME ve Web

MIME (Multipurpose Internet Mail Extentions – Çok Amaçlı İnternet Posta Eklentileri), Web üzerinde bilgilerin sınıflandırılmasında kullanılır. Örneğin gönderilecek bilginin bir web sayfası mı yoksa bir dosya mı olduğunu belirlemek için MIME kullanılır. MIME, sade metin dışında farklı formatta veriler de gönderilmesine olanak tanır. MIME sayesinde ASCII olmayan, örneğin; ses, video, resim, uygulamalar gibi daha pek çok farklı veriler içeren web sayfalarını da gönderip alabiliyoruz.

Web Tarayıcı ve sunucu iletişim kurdukları zaman kullanacakları MIME çeşidi hakkında anlaşırlar. Tarayıcı istek başlığında kabul edebileceği MIME tipini sunucuya bildirir. Sunucu da göndermek üzere olduğu verinin MIME çeşidini kullanıcıya bildirir. Böylece anlaşırlar.

Aşağıda sık karşılaşılan genel MIME çeşitleri listelenmiştir.

MIME Çeşidi	Açıklama
Text/plain	Sade Metin (ASCII)
Text/html	HTML Kodları
İmage/gif	GIF Resmi
İmage/jpeg	JPEG Resmi
Application/msword	Microsoft Word Belgesi
Video/mpeg	MPEG Video
Audio/wave	Wave Ses
Application/x-tar	TAR - Sıkıştırılmış Veri

Tablo 13: Sık Karşılaşılan MIME Çeşitleri.

2.2.3.3. Örnek HTTP İletişimi

Buraya kadar sunucunun ve sunucuya bağlanan web tarayıcının birbirlerine neler söylediklerini, paylaşabilecekleri veri çeşitlerini gördünüz. Şimdi bu protokolün çalışmasına dair bir örnek verelim.

Tarayıcı İsteği:

Bu örnekte tarayıcı http://www.batl.k12.tr/index.html URL (Uniform Resource Locators – Tek biçimli Kaynak Göstericileri) ile tanımlanmış belge için istekte bulunuyor. Bütün istekler örnekte de gösterildiği gibi bir tane boş satırla biter.

```
GET/index.html HTTP/1.1
Accept: text/plain
Accept: text/html
User-Agent: Opera/9.10 (Windows NT 5.1; U; tr)
                  <Boş Satır>
```

Tarayıcı GET metodu ile /index.html dosyasını istiyor. Tarayıcı yalnızca sade metin ve html kodları alabileceğini ve Opera/9.10 (Windows NT 5.1; U; tr) tarayıcısı kullanıldığını belirtiyor.

Sunucu Cevabı:

Sunucu gelen isteğe durum kodu ile karşılık verir. Bu kodun hemen arkasından bir başlık ve başlığın arkasından bırakılan boş bir satırdan sonra istenilen belge içeriğini gönderir.

```
HTTP/1.1 200 OK
Date Wednesday, 28-Feb-07 15:49:21 GMT
Server: Apache/2.0
MIME–version: 3.0
Content–type: text/html
Last–modified: Thursday, 22-Feb-07 10:30:38 GMT
Content–length: 1453
  <Boş Satır>
<HTML>
<HEAD>
<title> Örnek Sunucu – Tarayıcı İletişimi </title>
</HEAD>
<BODY>
...
```

Şimdiki örnekte de olmayan bir belge (web sayfası) için yapılan isteğe karşılık gönderilen sunucu cevabıdır.

```
HTTP/1.1 400  NOT FOUND
Date Wednesday, 28-Feb-07 19:51:28 GMT
Server: Apache/2.0
```

Server-Side (Sunucu Taraf) Fonksiyonelliği

Web sunucuları tarayıcılara gönderebilecekleri geniş bir veri yelpazesine sahiptir. HTML sayfaları, video, ses ve resim bunlardan birkaçıdır. Bu veriler statik bir sayfadan veya dinamik bir sayfadan gönderilebilir. Dinamik sayfalarda, tarayıcı web sayfasına istekte bulunduğu anda gelen parametrelere göre kullanıcının isteğine uygun verileri seçerek bir sayfa üretilip kullanıcıya gönderilebilir. Dinamik sayfaların içerikleri sabit değildir. Dinamik sayfalar yapmak için birçok teknoloji kullanılabilir.

Common Gateway Interface (CGI)
Application Programming Interface (API)
Java Servlets
Server-Side JavaScript
Server-Side Includes

Bu teknolojilerden birkaçıdır.

2.2.3.4. SSL ve S-HTTP

Secure Socet Layer (SSL) ve Secure HTTP web üzerinden hassas verilerin gönderildiği iki protokoldür.

SSL Netscape Communications Corporation tarafından geliştirilmiştir. Özel bir şifreleme anahtarı ile hassas bilgileri güvenli bir şekilde gönderir. SSL tabanlı sunucular URL'de http yerine https protokolü kullanılarak belirtilir.

S-HTTP, http'nin özellikleri geliştirilmiş sürümüdür. Güvenli mesajlar göndermekle görevlidir. Bütün tarayıcılar ve sunucular S-HTTP'yi desteklemezler.

2.2.3.5. HTTP-ng

Gelecek nesil HTTP'dir (Next Generation). HTTP-ng adının uygun olacağı düşünülmüştür. HTTP-ng daha güvenli, daha hızlı olarak HTTP'nin yerini alacaktır. Daha fazla fonksiyonellik sunarak ticari uygulamalara daha uyumlu olacaktır. HTTP-ng ile birlikte gelecek yeniliklerden bazıları şunlardır:

- Geliştirilmiş modülerlik
- Geliştirilmiş ağ kararlılığı
- Geliştirilmiş güvenlik ve doğrulama
- Basit Yapılılık

Sonuç olarak bu bölümde, web sunucularını ve web tarayıcılarını inceledik, nasıl iletişim kurduklarını ve bilgileri nasıl gönderip aldıklarını gördük. Bu bilgileri gönderdikleri protokol olan HTTP/1.1'in özelliklerini ve nasıl iletim yaptığını öğrendik.

2.2.4. SMTP (Simple Mail Transfer Protocol)

Kişiden kişiye iletişim hayatın gerçeğidir. Aile bireylerimizle, arkadaşlarımızla, ve diğer kullanıcılarla iletişim kurarız. Kuşkusuz, bilgi çağı ile ortaya çıkan en önemli teknoloji elektronik postadır. Daha yaygın ismi ile e-posta. Milyonlarca insanın bilgisayarından birbirine gönderilmiş, şu anda da iletilmekte olan milyonlarca e-posta İnternet ortamında dolaşmaktadır. E-postalar, insanların değişen dünyadaki yeni iletişim biçimidir.

İnternet bilim adamları ile teknisyenlerin aralarında iletişim kurmak için geliştirdikleri bir sistemdi. Elbette e-posta bu iletişimde kullanılan ilk haberleşme yolu değildi. İnternet

yaygınlaştıkça E-posta ortaya çıktı ve aynı hızda yaygınlaştı. Fakat, e-posta'nın gelişim sürecinde internet üzerindeki en yaygın haberleşme aracı olmaktan çıkarak daha çok insanların birbirleri ile video, müzik gibi çoklu ortamların paylaşım aracı halini aldı. Artık e-posta yazılı mesajların yanında her türlü dosyayı iletir hale geldi.

E-postanın ilk dönemlerinde insanlar tek bir bilgisayara bağımlıydı. Be-postalar aynı bilgisayar üzerindeki farklı kullanıcıların birbirlerinin posta kutularına mesajların birer kopyasını bırakmalarından ibaretti. E-postanın ilk gelişimi LAN üzerinden başka bilgisayarlara postaların gönderilmesiyle gerçekleşti. Kısa bir süre sonra, kullanıcılara bir e-posta sunucusundan başka bir sunucuya posta gönderip almalarına olanak tanıyan ve Gateway olarak bilinen bir bileşen keşfedildi. Gateway'ler farklı e-posta sistemlerinin haberleşmelerini sağlamak üzere tasarlandı ve halen insanların birbirlerine gönderdikleri e-postaların belli standartlar dahilinde diğer sunuculara iletilmesini sağlamaktadır. Aslında iki çeşit e-posta standardı vardır. Bunlardan biri; International Telecommunications Union – Telecominications Standards Sector (ITU-TSS) ve ISO tarafından geliştirilmiş X.400, diğeri ise İnternet uzmanları tarafından geliştirilmiş ve Internet Engineering Task Force (IETF) standart kabul edilmiş SMTP'dir.

2.2.4.1. X.400

X.400 standardı, ilk olarak 1984 yılında ITU tarafından tanımlandı ve en son güncellemesi 1988 yılında yapılmıştır. X.400 çok güçlü ve karmaşık bir protokol yapısına sahipti. Bu karmaşıklığı nedeniyle dünya genelinde SMTP kadar kullanıcı bulamamıştır.

X.400'ün kullandığı iletim sisteminde bazı nitelik sembolleri vardır. Bu semboller, iletim koşullarını belirler. Bu semboller:

- Hassasiyet ve önem seviyesi
- Öncelik
- Geçerlilik süresi
- İletim ve alım bildirimi
- Tarihe göre yanıtlama

Nitelik	Açıklama
G	Adı
I	Göbek adı
S	Soyadı
Q	Unvanı
CN	Şirketin Genel İsmi
O	Şirket
OU	Şirket İçi Bölüm
P	Özel Yönetim Domain'i
A	Yönetimsel Kontrol Domain'i
C	Ülke

Tablo 14: X.400 Adres Bileşenleri

X.400'ün mesaj yapısı gibi adres yapısı da karmaşıktır. Tablo 2.8'de X.400 adresini oluşturan nitelikler ve anlamları listelenmiştir.

Örnek X.400 alıcı adresi; C=TR;A=XXX;P=BATL;O=MEB;OU=EGT;S=SULAK; G=Mirhac; olarak tanımlanır. Bu örnekte, ülkem Türkiye (C=TR); yönetimsel domain'im veya kullandığım X.400 servisini sağlayan sunucu XXX (A=XXX); çalıştığım bölüm Bilgisayar Anadolu Teknik Lisesi (P=BATL); işveren kurum Milli Eğitim Bakanlığı (O=MEB); bölümün alanı Eğitim (OU=EGT) kalanlar ise isimdir.

Şimdi bu adres yapısını bir de admin@batl.k12.tr SMTP adresi ile karşılaştırın. Sizce hangisi daha kullanışlıdır?

2.2.4.2. SMTP

SMTP (Basit Posta İletim Protokolü) internetin e-posta standardıdır. İki bilgisayar arasında öncelikli olarak İnternet ve ağlar üzerinden posta iletimi yapan bir uygulama katmanı protokolüdür. Temel işlevi posta göndermektir. Mesajın içeriği yada düzenlenmesi ile ilgilenmez. Yalnızca mesajı bil bilgisayardan diğerine taşımakla görevlidir.

İki bilgisayardan birisi SMTP alıcı, diğeri ise SMTP gönderici olarak görevlendirilir. Alıcıdan göndericiye mesaj üç aşamada iletilir.

- TCP bağlantısı kurulur,
- Veri aktarımı ile mesaj gönderilir (data transfer)
- Bağlantı kapatılır.

Bütün işletim sistemlerinin hemen hepsinde SMTP kullanan e-mail client uygulaması vardır. Aynı zamanda SMTP server uygulaması da mevcuttur. Örneğin; Windows 9x/NT/2000/XP/2003/Vista, MacOS, Unix ve türevleri, Linux, BeOS ve hatta AmigaOS SMTP server uygulamasına sahip işletim sistemlerine örnektir.

SMTP e-posta mesajlarını çok çeşitli ağlar altında dahi iletebilmek için tasarlanmıştır. Aslında postacı gibi çalışır. Mesajın ne olduğuyla ya da nasıl gittiğiyle ilgilenmez. Sadece mesajı hedefine ulaştırır.

SMTP, belirgin kriterler üzerine kurulmuş otomatik posta yönlendirmelerine olanak tanıyan çok güçlü posta yönetim özelliklerine sahiptir. SMTP, e-posta adresi bulunamazsa, kullanıcıyı anında haberdar eder. Sistem yöneticisi tarafından belirlenen zaman aşım süresi dolduktan sonra iletilemez duruma gelen e-postayı gönderici adrese teslim eder.

SMTP 25 numaralı TCP portunu kullanır. TCP segmentleri ile ileti taşıması yaptığı için güvenilir ve garantili bir iletim sunar.

MIME ve SMTP

MIME bir SMTP eklentisidir. SMTP mesajlarının içerisine çoklu ortam (metin olmayan) dosyalarını dahil ederek kodlar. MIME base64 kodlama sistemini kullanarak karmaşık dosyaları 255 karakterlik ASCII karakter setine dönüştürür.

MIME yeni bir standart olmasına rağmen neredeyse bütün e-posta uygulamaları tarafından desteklenmektedir. Eğer uygulamanın bu standardı desteklemiyorsa BinHex veya

uuencode gibi farklı bir kodlama metodu kullanmalısınız. Bunların dışında da pek çok kodlama sistemi mevcuttur.

S/MIME

MIME için yeni bir özelliktir. Şifrelenmiş mesajları okumamızı sağlar. S/MIME, RSA (Rivest, Shamir and Adleman algoritması) genel şifreleme tekniği üzerine kurulmuştur. Mesajların ele geçirilmesi ve taklit edilmesini engeller.

SMTP Komutları

SMTP'nin diğer bir kolaylığı da az sayıda komut kullanarak iletim yapmasıdır. SMTP'nin kullandığı komut seti şunlardır:

KOMUT	AÇIKLAMA
HELO	Hello, Alıcaya, göndericiyi tanımlamak için kullanılır. Bu komut, gönderici host ismi ile birlikte olmalıdır. Genişletilmiş (ESMTP) protokolde EHLO komutu kullanılır.
MAIL	Posta gönderimini belirtir. "Kimden" veya gönderici alanını içerir.
RCPT	Posta alıcısını tanımlar.
DATA	Asıl Posta içeriğinin başladığını belirtir.
RSET	Gönderimi keser.
VRFY	Alıcı tarafından alındığını onaylamak için kullanılır.
NOOP	"NoOperation" herhangi bir işlem yapılmadığını gösterir.
QUIT	Bağlantıyı sonlandırır.
SEND	Alıcı bilgisayara, mesajın başka bir terminal bilgisayara gönderilmesi gerektiğini bildirir.
SOML	Alıcı bilgisayara, mesajın başka bir terminal veya posta kutusuna gönderilmesi gerektiğini bildirir.
SAML	Alıcı bilgisayara, mesajın başka bir terminal ve posta kutusuna gönderilmesi gerektiğini bildirir.
EXPN	Alıcı listesini genişletmek için kullanılır.
HELP	Alıcı bilgisayardan yardımcı olabilecek bilgiler göndermesi için istekte bulunur.
TURN	Alıcı bilgisayarın gönderici bilgisayar rolünü üstlenmesi için istekte bulunur.

Tablo 15: SMTP Komut seti.

SMTP Durum Kodları

Gönderici uygulama SMTP komutları ile e-posta gönderdiği zaman, alıcı uygulama özel durum kodlarıyla gönderici tarafı bilgilendirir. Aşağıdaki tabloda bu durum kodları gruplandırılarak listelenmiştir.

KOD	AÇIKLAMA
211	Yardım cevabı, sistem durumu
214	Yardım mesajı
220	Servis hazır
221	Bağlantı kapatılıyor
250	İstenilen işlem kabul edildi
251	Kullanıcı aynı ağda değil, mesaj <….>'ya iletiliyor
354	Mesaj içeriğini göndermeye başla
421	Servis kullanılamaz
450	İstek alınamadı, posta kutusu meşgul
451	İstek iptal edildi, yerel hata
452	İstek alınamadı, yetersiz depolama alanı
500	Komut tanımlanamadı veya hatalı komut dizilimi
501	Parametre veya değişkenlerde yazım hatası
502	Komut desteklenmiyor.
503	Komut sıralaması hatalı.
504	Komut parametresi desteklenmiyor.
550	İstek alınamadı, posta kutusu kullanılamaz.
551	Yerel kullanıcı değil.
552	İptal edildi: Depolama sınırı aşıldı.
553	İşlem iptal edildi, posta kutusu ismi kullanılamaz.
554	İletim başarısız.

Tablo 16: SMTP Durum Kodları

500 ile başlayan kodlar transferde başarısızlık, 400'lü kodlar geçici sorunlar için, 100-300 arası kodlar ise başarılı transferler içindir. Örnek bir SMTP posta gönderim komut dizilimi oluşturarak bu kodların nasıl kullanıldığına bakalım.

220 aliciadres.com
---- Server ESMTP Sendmail 8.8.8+Sun/8.8.8; Cum, 28 Sub 2007 08:53:21 HELO mail.gondericiadres.com
250 aliciadres.com Merhaba mail.gondericiadres.com, tanıştığımıza memnun oldum
---- MAIL FROM:<gonderen@gondericiadres.com>
250 <gonderen@gondericiadres.com> Gönderici Tamam.
---- RCPT TO: <alici@aliciadres.com>
250 <alici@aliciadres.com> Alıcı Tamam
---- DATA

354 Posta içeriğini gönder, tek başına “i,î” olan bir satırla sonlandır.
---- Mesaj burada gönderiliyor…
---- …….
250 Mesaj dağıtım için kabul edildi.
---- QUIT
221 Güle güle mail.gondericiadres.com

İletilen e-posta mesajı aşağıdakine benzer bir şekilde olacaktır.

From: gonderici@gonderici.com 28 Şub 2007 08:53:21
Tarih: Cuma, 28 Şub 2007 08:53:21 +02:00 (GMT)
From: gonderici@gonderici.com
Mesaj-id: <200702280653.JAA13734@mail.aliciadres.com>
İçerik-Uzunluğu: 23
Mesaj buradan başlıyor…

Yukarıda da gördüğünüz gibi her komuta karşılık ürettiği durum kodlarının yanında göndericiye bir de parametre şeklinde açıklama gönderiliyor. Bu durum bilgilerine göre gönderici mesaj gönderme işlemini gerçekleştiriyor.

Gönderilen mesajların TCP ve UDP başlıkları gibi bir de SMTP başlığı vardır. Bu başlık iletim protokollerininkiler gibi karmaşık değildir. Bir SMTP başlığına bakarak mesajın kimden geldiği, kimlere gönderildiği, mesajın konusu, tarihi gibi bilgileri alabilirsiniz. SMTP başlığının içermek zorunda olduğu asgari bilgiler şunlardır: Gönderici (FROM) , tarih ve alıcı adresi (TO, CC veya BCC).

FROM : Gönderenin Adresi.
DATE : Tarih
SUBEJCT : Konu
TO : Alıcı veya Alıcıların Adresi (alıcı tarafta görüntülenir)
CC : Bilgisine Sunulan Kişi veya Kişilerin Adresleri (Alıcı tarafta görünür)
BCC : Gizli Alıcı veya Alıcıların Adresleri (Alıcı tarafta görüntülenmez)

Gönderilen iletilerde, alıcılarda görüntülenmesini istemediğimiz adresler BCC (Gizli) kısmına yazılmalıdır.

SMTP’nin Avantaj ve Dezavantajları

Avantajları:
- SMTP çok yaygındır.
- Birçok platform ve servis sağlayıcı tarafından desteklenir.
- SMTP uygulama ve yönetim maliyeti çok düşüktür.
- SMTP’nin basit bir adres şeması vardır.

Dezavantajları:
- SMTP’nin belirgin fonksiyon tipleri yoktur.
- SMTP, X.400’ün güvenlik özelliklerinden yoksundur.

- Sadeliği, kullanışlılığını sınırlandırmaktadır.

2.2.5. SNMP (Simple Network Management Protocol)

SNMP (Basit Ağ Yönetim Protokolü) ağ üzerinde bulunan ağ elemanları hakkında bilgi toplamak için geliştirilmiş bir protokoldür. Ağ cihazlarının uzaktan kontrol edilmesini ve uzaktan bu cihazlara müdahale edilmesini sağlar.

İnternet yaygınlaştıkça genişlemekte ve küçük ağlar birleşerek internetin bir parçası olmaktalar. Bu ağların birleşmesini sağlayan yönlendiriciler (router), köprüler (bridge) gibi önem kazanan ağ elemanlarının ağları nasıl birleştireceklerinin belirlenmesi, ayarlarının yapılması, sağlıklı çalışıp çalışmadıklarının izlenmesi, bu işlemlerin de uzaktan yapılması önem kazandı.

SNMP ile bu cihazları kontrol edebilir, bu cihazın bağlantıya izin vereceği portları, hangi bilgisayarların ağa ya da internete bağlanacaklarının kontrolünü yapabiliriz.

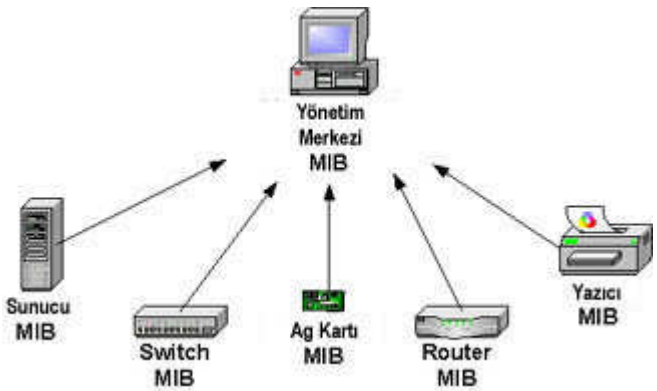
Bununla birlikte SNMP ile bütün bir ağı yönetebilir ve kontrol edebiliriz. DHCP'nin kaç bilgisayara IP adresi dağıttığını, hangi bilgisayarların ağa bağlandığını, bu bilgisayarların ne kadar veri transferi yaptığını takip edebiliriz.

Bu işlemleri yapabilmek için ağ üzerinde çalışan aygıtlarda bu aygıtların yönetilebilmesini sağlayan gerekli uygulamalar bulunur. Bu uygulamalar sayesinde aygıtlar kontrol altında tutulabilir ve takip edilebilirler.

2.2.5.1. SNMP'yi Oluşturan Bileşenler

SNMP, biri ağ elemanında, diğer ikisi de yönetim merkezinde olmak üzere üç temel bileşenden oluşur.

- **Ajan Uygulama:** Cihaz üzerinde çalışır, gerekli bilgileri kayıtlı tutarak yönetici birime aktarır. Aynı zamanda yönetici birimden gelen değişiklikleri de cihaza uygular.
- **Yönetici Uygulama:** Ajan uygulamadan bilgileri alır kullanıcıya gösterir ve kullanıcının değiştirmek istediği değerleri de cihaza gönderir.
- **Ağ Yönetim Sistemi (NMS):** Yönetici birimde çalışır. Bir ağa bağlı tüm cihazların izlenmesini ve yönetimini sağlar.



Şekil 19: SNMP Yönetim Sistemi.

Bir SNMP yönetici uygulama, ağ birimleri üzerinde bulunan ajanları sorgulayarak ağ ile ilgili bilgileri toplar. Bu işlemin ardından, ağa ilişkin analizleri yapabilmesi için bu bilgileri ağ yönetim sistemine gönderir.

SNMP de bir protokoller grubudur. Bu protokol grubunda yer alan protokoller şunlardır.

- Structure and Identification of Management Information (SMI)
- Management Information Base (MIB)
- Simple Network Management Prokocol (SNMP)

2.2.5.2. Yönetim Bilgilerinin Yapı ve Tanımlamaları (SMI)

Ağla ilgili bilgilerin kaydedildiği veritabanının ajan yapısını belirler. Bir veri tabanı oluşturmak için öncelikle bu veritabanının yapısının nasıl olacağına karar verilmelidir.

2.2.5.3. Yönetim Bilgi Tabanı (MIB)

Bir MIB herhangi bir SNMP veritabanında bulunan nesneleri ve girişleri tanımlar. Kısaca MIB ağ elemanları üzerinde bulunan, bu elemana ait bilgilerin bulunduğu bir tablodur. Standart, deneysel ve özel olmak üzere üç MIB kategorisi vardır.

Standart MIB: Internet Standart Group tarafından onaylanmış nesneleri içerir. İlk standart MIB'ler olan MIB I ve MIB II, IP routerleri yönetmek için geliştirildi. RMON (Remote MONitoring) MIB I, Internet topluluğu tarafından standart bir MIB olarak onaylanmiştir. RMON'un MIB II ye göre biraz farklı bir amaç için tasarlanmıştır. RMON'un içinde, ağ iletim ortamını izlemek için gerekli nesneler vardır. RMON MIB I ile bir ağ segmentindeki paket trafiği, segment kullanım oranı, hatalı paket sayısı hakkında bilgiler edinilebilir. Aynı zamanda RMON ile SNMP ajanı bulunmayan birimler de izlenebilir.

Deneysel MIB: Bu sınıftaki MIB'lerde ağ ve ağ birimlerinin yönetimi için saha çok bu birimlere özel, diğer MIB'lerde bulunmayan tanımlamalar vardır.

Özel MIB: Bu MIB'ler ağ üzerine çalışan şirketler tarafından geliştiriliyor ve üreticinin kendi ağ birimlerine özel bilgiler toplamak amacıyla kullanılıyor. Bu MIB'lerde nesneler, üretici tarafından tanımlanırlar.

MIB'ler gelişi güzel hazırlanmaz. Ağ üzerine çalışan firmalar ya da bağımsız kuruluşlar tarafından hazırlanır ve International Standards Organization (ISO) Uluslar arası Standartlar Organizasyonu tarafından onaylanır. Onaylanırken her MIB'e bir nesne adı ve bir de nesne numarası verilir.

Nesne adı: iso.org.dod.internet.mgmt.mib-2.system.sysDescr
Nesne Numarası: 1.3.6.1.2.1.1.1

Nesne adı: iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber
Nesne Numarası: 1.3.6.1.2.1.2.1

Nesne isimlerinde ve numaralarında dikkat edilirse ortak olan kısımlar var. Nesneler numaralandırılırken belli bir hiyerarşiye göre numara verilir. Bu aynı tür göreve sahip nesnelerin bir grup oluşturmasını sağlar.

MIB İsim Kodu	No
ISO (Uluslar arası Standartlar Orghanizasyonu)	1
Organization	3
Department Of Defense (USA-DOD) (ABD-SB)	6
Internet	1
Directory	1
Management	2
Experimental	3
Private	4
MIB II	1
Enterprise	1
Ajana özel numara	--

Tablo 17: MIB Numaralandırma Grupları.

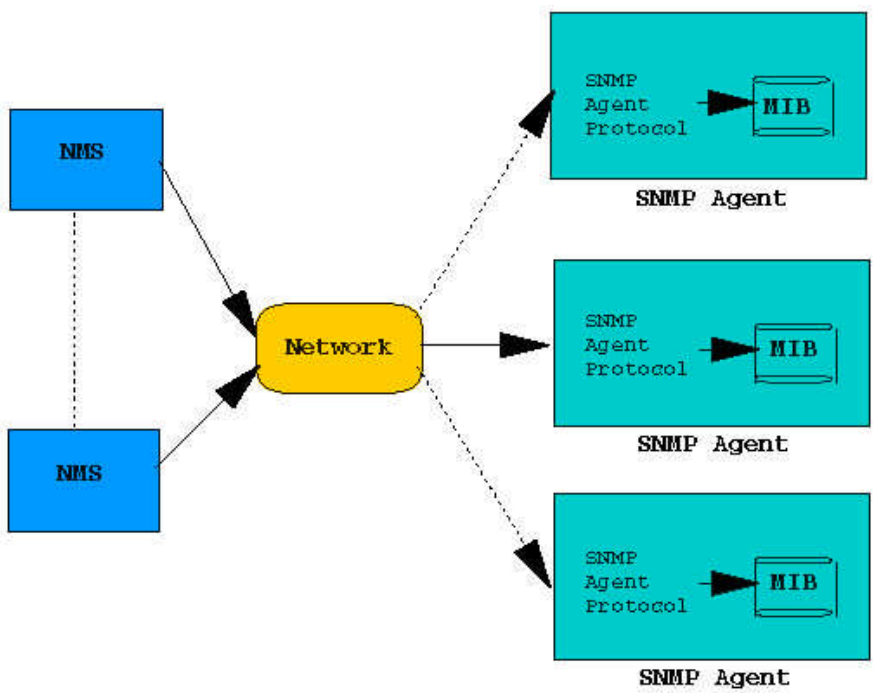
2.2.5.4. Basit Ağ Yönetim Protokolü (SNMP)

Herhangi bir ağ yönetim uygulamasının SNMP MIB'lerini sorgulayabilmesi için tasarlanmış olup üç versiyonu vardır. İlk versiyon SNMPv1 dört temel işlemi gerçekleştirirken v2 ve v3 sürümlerinde birer işlem daha eklenerek toplamda altı farklı işlem yapabilen bir client/server protokolü haline gelmiştir. SNMP bu işlemleri gerçekleştirmek için önce bir istek gönderir ardından bu isteğe cevap bekler. İsteğe karşılık olarak ağ

elemanındaki ajan uygulamadan bilgiler gelir. Bu bilgilerin iletimi için UDP ve IP protokolleri kullanılır.

Aşağıda sıralanmış ilk dört komut v1, son iki komut ise v2 ve v3 sürümleri ile gelmiştir.

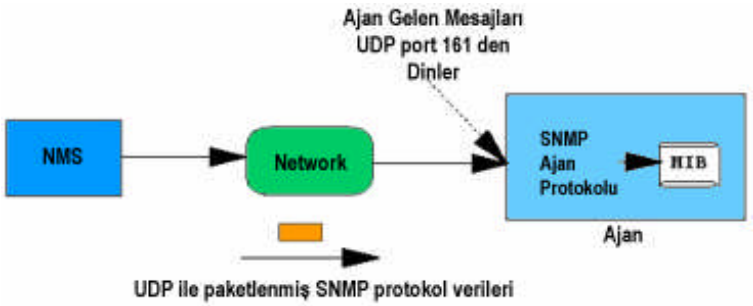
- **GET :** Yönetilen ağ elemanından bir bilgiyi almak için kullanılır.
- **GET-NEXT :** Ağ elemanından bir sonraki bilgiyi çağırarak bilgi tablolarını taramak için kullanılır.
- **SET :** Yönetilen cihaz üzerindeki bir bilgiyi değiştirmek için kullanılır.
- **TRAP :** Önemli olayların (eşik değeri ayarlanmış) yönetim uygulamasına rapor edilmesi için kullanılır. Bu işlem için yönetim uygulama programından herhangi bir istek gelmesi gerekmez
- **GETBULK:** Bilgiler önceki sürümde tek tet alınırken 2. sürümde bu işlem sayesinde gönderilen tek bir istekle tablolardan aynı anda birkaç sütun bilgi almak mümkün olmuştur.
- **INFORM:** Üçüncü sürümde bu işlemle bir yönetim sisteminin bir diğer yönetim sistemini bilgilendirebilmektedir.



Şekil 20: SNMP Mimarisi.

SNMPv2: Bu protokol Internet topluluğu tarafından onaylanmış bir yönetim protokolü olup SNMPv1'in yeteneklerini arttırmak için geliştirilmiştir. Bu protokole geliştirilmiş güvenlik ve Router tablolarının tamamını sorgulayabilen GET-BULK komutu eklenmiştir.

SNMPv3: Bu sürüm de yönetim istasyonları arasında iletişimin sağlanması için geliştirilmiştir. Yönetim istasyonları arasında bilgi koordinasyonunu sağlayan INFORM komutu eklenmiştir.



Şekil 21: SNMP – ajan iletim modeli

SNMP mesaj göndermek için **UDP** iletim protokolünü kullanır. Bildiğimiz gibi, UDP güvensiz bir iletim protokolüdür.

Her ne kadar v1'in geliştirilmesi sonucu ortaya çıkmış olsalar da bu iki sürüm birbiriyle uyumlu değildir. Fakat her iki sürümü de destekleyen sistemler vardır.

2.2.5.5. SNMP Kullanım Alanları

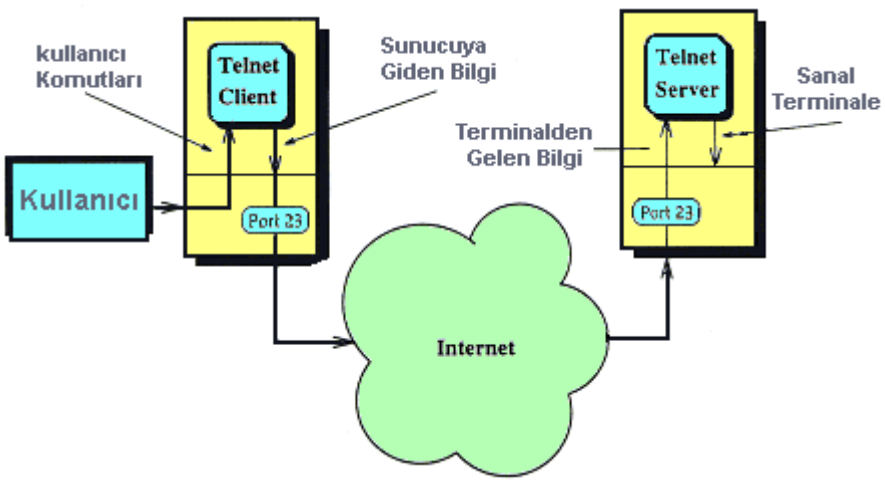
Büyük ağ sistemlerinde ağ cihazları yetkili kişiler tarafından kurulan ve ayarlanan büyük cihazlardır. Bu cihazlara bilinçsiz kişilerin müdahale etmemeleri ve cihazların etkin bir biçimde çalışmaları için özel odalar ya da kabinlerde muhafaza edilirler. Bu sistemlerde oluşabilecek bir sorun ya da daha verimli çalışabilmeleri için gerekli düzenlemelerin yapılabilmesi için cihazları ayarlamak gerekebilir. Bu nedenle cihaza dokunmadan uzaktan bir bilgisayar aracılığı ile cihazı ayarlamak gerekir. Cihazın ayarlarının yapılabilmesi için cihaz içerisinde cihazla ilgili bilgileri tutan bir program (ajan) bulunur. Tüm ağ elemanları üzerlerinde bulunan bu programlarla uzaktan yönetilebilir.

SNMP büyük ve uzaktan yönetilme zorunluluğu olan bu ağ elemanlarının tek bir merkezden gözlenmesi ve ayarlanmasını sağlar. Sunucular (server), routerlar, modemler ve kişisel bilgisayarlar gibi ağı oluşturan birimlerin hepsinde birer SNMP ajanı bulunur. Bu ajanlar ağ yönetici uygulama programının isteği üzerine kendileri hakkında bilgileri gönderirler. Aynı zamanda oluşan herhangi bir acil durumu da yönetim merkezine bildirip sorundan yöneticinin haberdar olmasını sağlarlar.

2.2.6. Telnet

Telnet, TELecommunications NETwork teriminin kısaltılmasıdır. Hem uygulama hem de protokolün kendisidir. Aynı isim her ikisi için de geçerlidir. TELNET kullanıcıya ağ üzerinden doğrudan sunucu erişimine izin verir. Kısaca TELNET, uzak sunucu bilgisayara doğrudan erişim sağlar. TELNET 23 numaralı port üzerinden hizmet verir.

TELNET ile kullanıcı uzaktaki sunucuya bağlanıp orada bir uygulamayı çalıştırabilir. TELNET ile bağlantı yapabilmek için iki yazılıma ihtiyaç vardır.



Şekil 22: Telnet Bağlantı Şeması.

- Client (terminal) – TELNET
- Server (sunucu) – TELNET

Client yazılımı kullanıcının bilgisayarında çalışan bir uygulama programıdır. Bu uygulama TELNET sunucusuyla iletişim kurmayı sağlar. İletişim TCP ile yapılır.

Şekil 23: Telnet Kullanımı

TELNET, bağlanılmak istenen sunucu bilgisayarda yüklenmiş ve çalışır vaziyette olması gerekmektedir. Bu uzak sunucuya bağlanmak için öncelikle yetkilendirilmiş bir giriş oturumu açılması gerekir. Windows 9x / NT / 2000 / XP, BeOS, Linux ve diğer x86 platform tabanlı işletim sistemlerine uzaktan gelen bağlantıları kabul edemezler. Bu sistemlere uzaktan bağlanabilmek için TELNET sunucusun bu işletim sistemleri üzerine kurulmuş, ayarlanmış ve çalışır durumda olmak zorundadır. MacOS tabanlı işletim sistemleri de aynı şekilde server kurulumuna ihtiyaç duyar. Fakat Unix tabanlı işletim sistemleri buna ihtiyaç duymazlar. Sadece UNIX işletim sistemleri telnetd adlı bir TELNET sunucu uygulamasıyla birlikte gelir. Bağlanan tarafta ise, sunucuda bir oturum açabilmek için sadece arayüz olarak metin tabanlı veya grafik tabanlı (GUI) bir TELNET uygulaması bulunması yeterlidir.

Windows 2000 ve sonraki sürümlerinde TELNET Client uygulamasını bünyesine almıştır. Başlat - Çalıştır seçeneğinden “telnet” yazarsanız ya da bir telnet linkine tıklarsanız uygulama çalışacaktır.

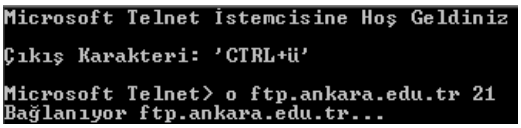
www yaygınlaşmadan önce kullanıcılar TELNET bağlantısı ile iletişim kuruyorlardı. Fakat günümüzde www yaygınlaştığı için TELNET artık eskisi kadar kullanılmıyor.

Komut	Açıklama	
open	Ana bilgisayar ile bir Telnet bağlantısı kurmak için, “open anabilgisayaradı” şeklinde kullanılır.	
close	Varolan bir Telnet bağlantısını kapatmak için kullanılır.	
display	Telnet İstemcisi için geçerli ayarları görüntülemek için kullanılır.	
send	Telnet sunucusuna komut göndermek için kullanılır. Ayrıca aşağıdaki komutları destekler:	
	ao	Çıktı komutunu durdurur.
	ayt	"Orada mısın?".
	esc	Geçerli çıkış karakterini ayarlar.
	ip	İşlem komutunu keser.
	synch	Telnet synch (eşitleme) işlemini gerçekleştirir.
	brk	Kesme sinyali gönderir.
	Yukarıdaki komutlar dışında send komutu ile gönderilen herşey bir metin olarak algılanır ve ekrana aynen yansıtılır. Örneğin send meb ekrana “meb” yazacaktır.	
quit	Telnet İstemcisi'ni kapatmak için kullanılır.	
set	Telnet İstemcisi'ni geçerli oturum için yapılandırmak üzere, set komutunu aşağıdaki değişkenlerden biriyle kullanın.	
unset	Daha önce set komutu kullanılarak ayarlanan bir seçeneği kapatmak için kullanılır.	
status	Telnet İstemcisi'ni çalıştıran bilgisayarın bağlı olup olmadığını belirlemek için kullanılır.	
?/help	Yardım bilgilerini görüntüler.	

Tablo 18: TELNET Komutları.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Öncelikle web tarayıcınızı açın. Bir FTP sitesinin adresini adres bölümüne yazın. Örneğin ftp://ftp.ankara.edu.tr	➢ FTP kullanabilmek için iki yol vardır. Kullanmakta olduğumuz web tarayıcı ile bir FTP sunucusuna bağlanabiliriz ya da bir FTP yazılımı ile FTP sunucularından rahatlıkla dosya alış-verişi yapabiliriz.
➢ Web tarayıcınızın ekranında klasör yapısı gelecektir. Bu ekrandan istediğiniz gibi dosya indirebilirsiniz.	➢ Eğer FTP sunucusu "Public" (herkese açık) ise doğrudan, eğer public değilse kullanıcı adı ve şifre soracaktır. Public FTP sunuculardan genellikle dosya indirilebilir. Upload yapılmasına izin verilmez.
➢ Tarayıcı ekranınızdan bir klasöre girip dosya kopyalayın, kendi bilgisayarınızda bir konuma geçip yapıştırın.	➢ Kendi klasörlerinizde gezinti yapar gibi FTP sunucu klasörlerinde gezebilirsiniz. Kopyala-yapıştır yöntemiyle dosya indirebilirsiniz.
➢ Dosyanın indirilirken komut satırından "netstat 1.5" komutu kullanarak bağlantı durumuna bakın.	➢ FTP bağlantının hangi aşamalarla kurulduğunu ve nasıl kapadığını görebilirsiniz.
➢ FTP kullanarak dosya transferi yapmış oldunuz.	
➢ TFTP kullanmak için ağ bağlantılarınıza girin. Dosya alacağınız bir bilgisayar seçin.	➢ TFTP genellikle yerel ağ içi dosya transferlerinde kullanılır. Ağınıza bağlı başka bir bilgisayardan dosya almalısınız
➢ Karşı bilgisayarın paylaşıma açık klasörlerine girin ve bir dosya kopyalayın.	➢ Paylaşıma açık olmayan dosyalara erişim izniniz olmayabilir.
➢ Kendi bilgisayarınızda bir konuma bu kopyaladığınız dosyayı yapıştırın.	➢ Yapıştırma işleminde dosya diğer bilgisayardan TFTP protokolü ile UDP kullanılarak alınmaya başlar.
➢ Bilgisayarınızda TELNET client uygulamasını çalıştırın. (Başlat – Çalıştır – TELNET)	➢ Telnet uygulaması Windows işletim sistemlerinde standart olarak gelmektedir.
➢ Telnet komut satırında o ftp.ankara.edu.tr 21	➢ Ankara Üniversitesi FTP sunucusuna 21 numaralı FTP kontrol portu kullanarak bağlantı yapmış olursunuz.

	
 ➢ USER anonymous yazın	➢ Anonymous herkese açık bir kullanıcı adıdır. Fakat hakları sınırlıdır.
➢ PASS sifre yazın	
➢ FTP sunucusuna kısıtlı haklarla bağlandınız. PWD yazın ve bulunduğunuz dizini görün.	➢ O anda içinde bulunduğunuz dizini gösterir.
➢ CWD /debian yazın ve "debian" dizinine girin.	➢ PWD yazarak içinde bulunduğunuz konuma tekrar bakabilirsiniz.
➢ QUIT yazın ve FTP bağlantısını kapatın.	➢ FTP bağlantısı kapanacak fakat TELNET ekranında kalacaksınız.

Öğretmeninizin ayrıca vereceği önerileri uygulama tablosuna not ediniz.

ÖLÇME VE DEĞERLENDİRME

Bu bölümde birinci öğrenme faaliyetinde verilen bilgilere hakimiyetinizi ve konuyu kavrama düzeyinizi ölçecek sorular sorulacaktır. Soruları bu düşünce doğrultusunda cevaplayınız.

OBJEKTİF TEST (ÖLÇME SORULARI)

Aşağıda verilen sorular için uygun cevap seçeneğini işaretleyiniz.

1. Aşağıdakilerden hangisi uygulama katmanı protokollerinden biri değildir?
A) SMTP
B) DNS
C) SNMP
D) UDP

2. Aşağıdakilerden dosya iletimi için kullanılan protokolüdür?
A) FTP
B) UDP
C) TELNET
D) SNMP

3. Uygulama katmanı hakkında aşağıdakilerden hangisi doğru değildir?
A) Kullanıcıya en yakın katmandır.
B) Uygulama programları bu katmanda çalışır.
C) Yalnızca gönderici tarafta bulunurlar.
D) İletilmesi istenen verileri taşıma katmanına önbellekler aracılığı ile iletirler.

4. DNS hakkında aşağıdakilerden hangisi yanlıştır?
A) Kullanıcının girdiği internet adresinin IP adresi karşılığını verir.
B) Bütün DNS sunucu kayıtları elle girilir.
C) Bütün DNS sunucularda internet ve IP adres kayıtları tutulur.
D) DNS sunucuları bölgesel olarak dağıtılmıştır.

5. SNMP hakkında aşağıdakilerden hangisi doğrudur?
A) Tamamen güvenli bir ağ yönetimi sağlar.
B) Ağ üzerinde çalışan cihazların uzaktan kontrolünü sağlar.
C) SNMP Ajanları ile ağ üzerindeki bilgisayarlardan her türlü bilgiyi alır..
D) Sadece ana bilgisayardan kontrol edilebilir.

6. FTP ve TFTP arasındaki fark aşağıdakilerden hangisidir?
A) FTP iletim için TCP kullanır, TFTP ise UDP kullanır.
B) FTP her türlü dosyayı iletir, TFTP yalnızca web sayfalarına ait dosyaları iletir.
C) FTP LAN üzerinde kullanıma uygun, TFTP internet üzerinde kullanıma uygundur.
D) FTP komutları daha azdır, TFTP ise daha çok komuta sahiptir.

7. İnternet üzerinde web sayfalarını görüntülemek için kullandığımız protokol aşağıdakilerden hangisidir?
A) SMTP
B) URL
C) HTTP
D) TELNET

8. Aşağıdakilerden hangisi SMTP protokolünün bir avantajı değildir?

A) Birçok platform tarafından desteklenir.
B) Çok yaygın bir protokoldür.
C) Basit bir adres şeması vardır.
D) Sadeliği ve basitliği kullanışlılığını arttırmaktadır.

9. MIME hakkında aşağıdakilerden hangisi yanlıştır?

A) E-posta içeriklerini yanlış kişilerin eline geçme ihtimaline karşı şifreler.
B) E-postalarda sade metin dışında farklı dosya türlerinin de iletilmesini sağlar.
C) E-postalarda gönderilecek bilginin türünü belirlemek için kullanılır.
D) Web üzerinde bilgilerin sınıflandırılmasında kullanılır.

10. Aşağıdakilerden hangisi TELNET için kullanılan port numarasıdır?

A) 21
B) 80
C) 23
D) 25

DEĞERLENDİRME

Sorulara verdiğiniz cevap seçeneklerini modül sonunda verilmiş olan cevap anahtarı ile karşılaştırınız. Kendinizi değerlendirdiğinizi unutmayınız. Yanlış cevapladığınız ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konular için bilgi sayfalarına tekrar dönerek eksiklerinizi gideriniz. Konu ilginizi çektiyse araştırma yaparak daha detaylı bilgi edinip kendinizi geliştirebilirsiz.

MODÜL DEĞERLENDİRME

Bu kısımda modül içerisindeki öğrenme faaliyetlerinde öğrendiğiniz bilgilerle ilgili, düşünce gücünüzü ölçecek sorular sorulacaktır. Bazı soruların cevaplarını hemen bulabilir bazılarını cevaplamanız ise zaman alabilir. Bu düşünce ile hareket ederek soruları cevaplayınız

OBJEKTİF TEST (ÖLÇME SORULARI)

Aşağıda verilen sorular için uygun cevap seçeneğini işaretleyiniz.

1. Aşağıdakilerden hangisi TCP/IP taşıma katmanının alıcı taraftaki görevlerinden biridir?
A) Kendisine gelen paketlere TCP başlıkları ekleyerek bir alt katmana iletmek.
B) Kedisine gelen paketlerden TCP başlığını çıkararak bir üst katmana iletmek.
C) Verileri segmentlere dönüştürerek göndermeye hazır hale getirmek.
D) Segmentlere verileri eklemek.

2. TCP protokolü segment yapısı hakkında aşağıdakilerden hangisi yanlıştır?
A) Başlık uzunluğu alanı segment içindeki verinin boyutunu gösterir.
B) Her segmentin bir numarası vardır.
C) Gönderilen segmentlerde onay numarası vardır
D) Segment yapısında bayraklar kullanılır.

3. TCP protokolünü güvenli kılan özelliği aşağıdakilerden hangisidir?
A) Paket yapısının düzenli olması.
B) Gönderilen segmentler için alıcıdan onay alması.
C) Hedef portla bağlantı kurması.
D) Segmentleri arka arkaya seri bir şekilde göndermesi.

4. Ses ve video görüntülerinin iletiminde sıklıkla kullanılan iletim protokolü hangisidir?
A) FTP
B) TCP
C) UDP
D) SNMP

5. Taşıma katmanı protokolleri, alıcı tarafta kendisine ulaşan bilgileri hangi katmana iletir?
A) Oturum Katmanı
B) Fiziksel Katman
C) İnternet Katmanı
D) Uygulama Katmanı

6. Aşağıdakilerden hangisi bir TCP portu değildir?
A) 20
B) 67
C) 25
D) 139

7. Aşağıdakilerden hangisi uygulama katmanının gönderici taraftaki görevlerinden biridir?
A) Kullanıcının karşı tarafa göndermek istediği bilgileri alt katmana iletmek.
B) Kullanıcının istediği dosyaları karşı tarafa taşımak.
C) Kullanıcının uygulama programlarını kontrol etmek.
D) Katman protokollerini denetlemek

8. Aşağıdakilerden hangisi internet üzerindeki bütün web sunucuların IP adreslerini ve bu IP adresleri ile eşleştirilmiş olan internet adreslerinin kayıtlı olduğu birimdir?

A) HTTP
B) TFTP
C) DNS
D) TELNET

9. Bir zamanlar çok popüler olan fakat günümüzde yaygınlığını büyük oranda yitirmiş iletişim protokolü aşağıdakilerden hangisidir.

A) DNS
B) TELNET
C) DHCP
D) SNMP

10. " …….. genellikle LAN üzerinde dosya transferi için kullanıma uygundur." ifadesinde boş bırakılan yere konulacak olan protokol ismi aşağıdakilerden hangisidir?

A) TFTP
B) HTTP
C) DNS
D) SMTP

DEĞERLENDİRME

Modül sonunda ilgili testlere ait cevap anahtarları bulunmaktadır. Bu cevap anahtarlarını kontrol ederek kendinizi değerlendirebilirsiniz. Yaptığınız değerlendirme sonucunda eksikleriniz varsa öğrenme faaliyetlerini tekrarlayınız.

Modülü tamamladınız, tebrik ederiz. Öğretmeniniz size çeşitli ölçme araçları uygulayacaktır. Öğretmeninizle iletişime geçiniz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1 CEVAP ANAHTARI CEVAP ANAHTARI

1	**C**
2	**B**
3	**C**
4	**B**
5	**D**
6	**A**
7	**C**
8	**D**
9	**B**
10	**A**

ÖĞRENME FAALİYETİ-2 CEVAP ANAHTARI CEVAP ANAHTARI

1	**D**
2	**A**
3	**C**
4	**B**
5	**B**
6	**A**
7	**C**
8	**D**
9	**A**
10	**C**

MODÜL DEĞERLENDİRME CEVAP ANAHTARI CEVAP ANAHTARI

1	**B**
2	**A**
3	**D**
4	**C**
5	**D**
6	**B**
7	**A**
8	**C**
9	**B**
10	**A**

KAYNAKÇA

- CARNE E. Bryan, **A Professional's Guide to Data Communication in a TCP/IP World**, Artech House Inc., London, 2004.
- FEIT Sidnie, **TCP/IP First Edition**, McGraw-Hill School Education Group, 1998
- RFC: 768 **USER DATAGRAM PROTOCOL**, Information Sciences Institute University Of Southern California, 1980
- RFC: 793, **TRANSMISSION CONTROL PROTOKOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION**, Information Sciences Institute University Of Southern California, 1981
- SIYAN Karanjit S. Ph.D., **PARKER Tim Ph.D**., Indianapolis, Sams Publishing, 2002
- STEVENS W. Richard, **TCP/IP ILLUSTRATED VOLUME1 THE PROTOCOLS**, Addison Wesley Professional, 1993.
- YILDIRIMOĞLU Murat, TCP/**IP INTERNET'İN EVRENSEL DİLİ**, Pusula Yayıncılık, 1999.
- www.bilgisayarogren.com/network7.doc
- http://computing-dictionary.thefreedictionary.com
- http://docs.sun.com
- http://www.nettica.com
- http://www.xincom.com/support/twr_user_guide/Chapter_7/